Implementing the Avaya B5800 Branch Gateway for an Avaya Aura® Configuration

Release 6.2
18-603853
Issue 3
October 2012

© 2012 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those product that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya is a registered trademark of Avaya Inc.

Aura is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: B5800 Branch Gateway overview 13
- PSTN trunking configurations 13
- Voicemail support options 14
- Management 14
- About upgrading B5800 Branch Gateways 16
- Licensing 16
- B5800 Branch Gateway licenses 18
- License modes 19
- System components 20
- Supported telephones 23
- Software applications 26
- Supported country locales 27
- New in this release 29
- Related resources 31
  - Related documents 31
  - Avaya Mentor videos 31
  - Training 31
  - Web sites 32
- Revision history 33

Chapter 2: Planning 35
- Prerequisites 35
- Dial plan considerations 36
- Dial plan example 36
- Voicemail considerations 37
- Branch PSTN call routing considerations 38
- Network assessment for VoIP requirements 39

Chapter 3: Installation requirements 41
- Power supply backup (UPS) 41
- Cables 42
- Grounding 44
- Wall and rack mounting 44
- Voice compression channels 44
- Emergency and power failure ports 46
- Environmental requirements 47
- Space requirements 48
  - Control unit 48
  - External expansion modules 49
  - Wall mounting space requirements 50
  - Rack space requirements 50

Chapter 4: Hardware and software installation 53
- Installation checklist 53
- Tools and equipment required 54
- Unpacking equipment 55
- SD card preparation 56

Upgrading the card firmware ... 56
Creating a configuration file ... 57
Adding a configuration file ... 58
Adding music-on-hold files ... 58
9600 series phones screen saver file ... 59
Base and trunk card installation ... 59
Trunk daughter card preparation ... 60
Legacy carrier card preparation ... 61
Base card insertion ... 63
Wall mounting ... 65
Rack mounting ... 67
External expansion modules ... 69
Connecting external expansion modules ... 70
Grounding ... 71
Out-of-building connections/lightning protection ... 72
DS phone IROB installation ... 74
Analog phone barrier boxes ... 75
Rack mounting barrier boxes ... 76
Administration software suite ... 77
PC requirements ... 78
Installing the administration applications ... 79
Installer PC connection ... 79
Connecting the PC directly to the control unit ... 80
Applying power to the system ... 81
Control unit LEDs startup sequence ... 82
About the LEDs ... 83
Default configuration ... 85
Connecting the control unit to the network ... 86
Connecting phones ... 87
Chapter 5: Upgrading an R6.1 system to R6.2 ... 89
Upgrade installation checklist ... 89
Upgrading the administration applications ... 90
Enabling secure communication after upgrading IP Office Manager ... 91
Exporting users to an xml file ... 92
Editing the xml file containing the users ... 92
Bulk importing of users ... 93
About migrating individual PLDS license files to a WebLM server ... 94
Deleting the PLDS license file from the branch ... 95
Chapter 6: Upgrading an R6.2 system with an R6.2 service pack ... 97
R6.2 service pack installation checklist ... 97
Remote Software Library for B5800 Branch Gateway upgrades ... 98
System requirements for the external server ... 98
Setting up the external server to work as a remote software library for B5800 upgrades ... 99
Getting inventory ... 100
Setting B5800 Branch Gateway SNMP attributes ... 100
Configuring user PLDS access ... 101
Creating a software library ... 102

Upgrading the B5800 Branch Gateway using System Manager 103
Chapter 7: Administration software suite 105
Starting System Status 105
Starting System Monitor 106
Chapter 8: Initial branch configuration 109
Configuration checklist 109
Setting up System Manager to launch IP Office Manager 112
Installing IP Office Manager from the System Manager server to a PC 114
Activating license files 115
Installing the shared PLDS license file on the System Manager WebLM server 117
Using Manager to deliver license files to the branches 117
Using Embedded File Management to install a PLDS license 118
Generating a certificate on System Manager 119
Using the Initial Installation Utility 121
Additional features configured by the Initial Installation Utility 123
Configuring the B5800 Branch Gateway for certificates 123
About adding B5800 Branch Gateways to System Manager 125
Discovering B5800 Branch Gateways 126
Bulk importing of devices 128
Adding the B5800 Branch Gateways to System Manager 129
Enabling WebLM licensing for the branch 130
Creating a system template 131
Uploading an auto attendant audio file 132
Applying the system template 132
Creating an endpoint template 133
Disabling unused trunks 134
Digital trunk clock source 135
Setting a trunk clock quality setting 136
Setting the trunk prefixes 137
SIP trunk prefixes 138
Administering a Session Manager line for each branch 139
Enabling SIP trunk support 139
Setting the branch prefix and local number length for extension numbering 140
Changing the default codec selection 143
Changing the maximum SIP sessions 144
Adding an Avaya Aura® Session Manager line 145
Avaya Aura® Session Manager line redundancy 150
Setting up outgoing call routing 151
How the B5800 Branch Gateway uses a configured Session Manager line 153
Enabling branch SIP extension support 154
SIP Registrar tab field descriptions 155
Chapter 9: Managing B5800 Branch Gateways from System Manager 157
Editing a B5800 Branch Gateway system configuration from System Manager 157
Restrictions when editing a B5800 Branch Gateway system configuration from System Manager. 158
About disabling the System Manager administration feature for a B5800 Branch Gateway 159
Disabling the System Manager administration feature for the branch from System Manager 160
Disabling the System Manager administration feature for the branch from IP Office Manager 160

Enabling the Security Settings option for the branch ... 161
Synchronizing B5800 Branch Gateway with System Manager ... 162
Configuration changes performed through Manager that cannot be synced with System Manager 162
Chapter 10: Session Manager Configuration ... 165
Viewing the SIP domains ... 166
Creating locations ... 166
Creating adaptations ... 167
Creating SIP entities ... 167
Creating entity links ... 168
Creating time ranges ... 169
Creating routing policies ... 169
Creating dial patterns ... 170
Chapter 11: Voicemail configuration ... 171
Voicemail options ... 171
About the Park and Page feature ... 172
Configuring Embedded Voicemail ... 173
Configuring Standalone Voice Mail ... 174
Configuring B5800 Branch Gateway to use Avaya Aura Messaging for voicemail ... 176
Configuring B5800 Branch Gateway to use Modular Messaging over SIP for voicemail ... 178
Modular Messaging and Avaya Aura Messaging PSTN Fallback ... 180
Adding an overriding short code ... 180
Uploading an auto attendant audio file ... 182
Chapter 12: User administration ... 185
Adding distributed users to System Manager ... 185
Editing the B5800 Branch Gateway Endpoint Profile for a user ... 187
Chapter 13: Managing license files with PLDS ... 189
PLDS Overview ... 189
Registering for PLDS ... 190
About license activation ... 190
Activating license entitlements ... 191
Searching for license entitlements ... 193
Moving activated license entitlements ... 195
Regenerate License files ... 197
Regenerating a license file ... 197
Chapter 14: Standalone SAL Gateway for remote service ... 199
Use of SAL to access the B5800 Branch Gateway administration tools and System Manager ... 199
SAL Gateway installation and registration ... 200
B5800 Branch Gateway registration and SAL Gateway on-boarding ... 201
B5800 Branch Gateway SAL-based alarming ... 201
Universal Install/SAL Registration Request Form ... 201
Chapter 15: Additional system procedures ... 203
Changing the IP address settings ... 203
Default passwords ... 204
Changing the security settings ... 204
Changing the remote user password ... 205
System shutdown ... 206
Shutting down the system using Manager ... 206

Shutting down the system using the System Status application ... 207
Shutting down the system using a system phone ... 207
Shutting down the system using the AUX button ... 207
Rebooting the system ... 208
About changing components ... 209
Replacing a component with one of the same type ... 209
Replacing a component with one of higher capacity ... 210
Replacing a component with one of lower capacity ... 210
Replacing a component with one of a different type ... 211
Adding a new component ... 211
Permanently removing a component ... 212
Swapping extension users ... 212
About changing extension numbers ... 213
Renumbering all extensions and users ... 213
Changing a user's extension number ... 214
Creating a backup of the system configuration using IP Office Manager ... 215
Creating a backup of the system configuration using System Manager ... 215
Upgrades using IP Office Manager ... 216
Using the upgrade wizard ... 217
Restoring the system configuration using System Manager ... 218
External output port (EXT O/P) ... 219
EXT O/P connections ... 220
Example of BRI So8 module configuration ... 221
Example 1: ISDN terminal ... 221
Example 2: video conference ... 222
SNMP ... 224
Installing the B5800 Branch Gateway MIB files ... 225
Enabling SNMP and polling support ... 228
Enabling SNMP trap sending ... 229
DTE port maintenance ... 230
RS232 DTE port settings ... 230
About erasing the configuration ... 231
Resetting the security settings to the default settings ... 234
Resetting the configuration and security settings to the default settings via the boot loader ... 234
About erasing the operational firmware ... 235
Reset button ... 238
Creating a WAN link ... 239
Chapter 16: SD card management ... 241
Booting from the SD cards ... 244
About creating a B5800 Branch Gateway SD card ... 246
Formatting an SD card ... 246
Formatting a System SD card using the System Status application ... 247
Recreating an SD card ... 247
Viewing the card contents ... 248
About backing up the System SD card ... 248
Backing up the primary folder using Manager ... 249
Backing up the primary folder using the System Status application ... 249

Backing up the primary folder using a system phone 250
About restoring from the backup folder 250
Restoring from the backup folder using Manager 250
Restoring from the backup folder using the System Status application 251
Restoring from the backup folder using a system phone 251
About backing up to the Optional SD card 252
Backing up to the Optional SD card using Manager 252
Backing up to the Optional SD card using the System Status application 252
Backing up to the Optional SD card using a system phone 253
About restoring from the Optional SD card 253
Restoring a configuration file from the Optional SD card using Manager 254
Restoring a configuration file from the Optional SD card using a system phone 254
Restoring software files from the Optional SD card using Manager 255
Restoring software files from the Optional SD card using a system phone 255
System upgrade using the System SD card 256
Upgrading remotely using Manager 257
Upgrading the SD card locally 257
Upgrading using an Optional SD card 258
Memory card removal 259
Shutting down a memory card using Manager 259
Shutting down a memory card using a system phone 260
Shutting down a memory card using System Status 260
Memory card startup 261
Starting up a memory card using Manager 261
Starting up a memory card using System Status 261
Starting up a card using a system phone 262
Chapter 17: Safety and regulatory information 263
Safety statements 263
Important safety instructions when using your telephone equipment 263
Lithium batteries 264
Lightening protection/hazard symbols 264
Trunk interface modules 265
Port safety classification 265
EMC cautions 266
Regulatory Instructions for Use 267
Australia 267
Canada 268
China 269
European Union 270
New Zealand 270
FCC notification 270
Compliance with FCC rules 272
Appendix A: Avaya port matrix for B5800 Branch Gateway and SIP phones 275
What are ports and how are they used? 275
Port type ranges 275
Sockets 276
Firewall types 277

Firewall policies ... 278
TFTP port usage ... 278
Ingress ports for B5800 Branch Gateway and SIP phones ... 279
Egress ports for B5800 Branch Gateway and SIP phones ... 281
Table column heading definitions ... 283
Port usage diagram ... 285
Appendix B: B5800 Branch Gateway call flows ... 287
Appendix C: Branch PSTN call routing examples ... 289
Centralized call control ... 289
Routing B5800 Branch Gateway calls — example ... 290
Branch PSTN override ... 292
Adding an overriding short code ... 292
PSTN trunk fallback ... 294
Configuring PSTN trunk fallback ... 295
Appendix D: Authorization codes ... 299
Enabling authorization codes in Manager ... 300
Force authorization codes ... 301
About entering an authorization code ... 301
Authorization code configuration settings ... 302
Appendix E: Recommended courses for Avaya B5800 Branch Gateway training ... 303
Recommended courses ... 303
Glossary ... 307
Index ... 309

Chapter 1: B5800 Branch Gateway overview

The Avaya B5800 Branch Gateway is a flexible, cost-effective communications platform for enterprise branch offices. It enables access via SIP to Avaya Aura® Session Manager in the enterprise center, optional access to centralized PSTN trunking, and access to centralized applications, such as conferencing, messaging, and more. The B5800 Branch Gateway solution provides centralized management by Avaya Aura® System Manager and centralized licensing by WebLM.

B5800 Branch Gateways are deployed in the distributed branch user model. In the distributed branch user model, call processing for the branch phones is provided locally. Non-IP phones are connected to the B5800 Branch Gateway and IP and certain SIP endpoints (not including the Avaya 9600 SIP phones) can be administered with B5800 Branch Gateway as their controller (see Supported telephones on page 23 for more information). Access to and from the rest of the Avaya Aura® network is via the B5800 Branch Gateway system's Avaya Aura® Session Manager link across the enterprise WAN. This connection allows for VoIP connectivity to other B5800 Branch Gateway systems, to centralized PSTN trunking, and to centralized applications such as conferencing and Avaya Aura® Messaging. The centralization capability is based primarily on the infrastructure at the enterprise core. The local B5800 Branch Gateway can be accessed as a SIP gateway connected to the core Avaya Aura®Session Manager to provide access to local PSTN trunks and services when required.

Beginning in R6.2, B5800 Branch Gateway is supported in an Avaya Communication Server 1000 (CS 1000) configuration. B5800 Branch Gateway can be deployed as a new branch in an existing CS 1000 configuration or as a replacement for Business Communications Manager (BCM) as a branch office in a CS 1000 branch office model. In these deployments, B5800 Branch Gateway operates as a distributed branch.

Note:

Integration of B5800 Branch Gateway with Communication Server 1000 is provided in a separate document. See *Implementing the Avaya B5800 Branch Gateway for a Communication Server 1000 Configuration*, document number 03-604053.

PSTN trunking configurations

With the ability to administer call control at both the B5800 Branch Gateway and the Avaya Aura®Session Manager, there are many ways you can optimize external PSTN trunk usage. The B5800 Branch Gateway is a full PABX and by default uses its own PSTN trunks. However it can be configured to make and receive external calls via the central Avaya Aura®Session Manager. A combination of these methods can be used for PSTN calls based on the call type

(local, national, international), time of day or even individual user. See Branch PSTN call routing examples on page 289 for more information.

Voicemail support options

B5800 Branch Gateway supports a range of options for voicemail services to the branch's native users. It supports Embedded Voicemail for native branch users and auto attendants to service local PSTN trunks. Standalone Voice Mail is also available for B5800 Branch Gateway systems when additional port capacity is required. Centralized voice messaging systems, Avaya Aura® Messaging or Modular Messaging over SIP, can also be configured. When using either of these centralized voice messaging systems, you are still able to use Embedded Voicemail or Standalone Voice Mail at each branch to provide auto-attendant operation and announcements for waiting calls. For more information, see Voicemail options on page 171.

Management

The primary method for configuring and managing the branches in a B5800 Branch Gateway system is centrally using Avaya Aura® System Manager R6.2. Avaya Aura® System Manager is a central management system that delivers a set of shared management services and a common console for different components of the Avaya Aura® solution. System Manager provides a single access interface to administer multiple branch locations and multiple distributed B5800 Branch Gateway users. System Manager also launches IP Office Manager in the appropriate mode where you can remotely administer individual B5800 Branch Gateways.

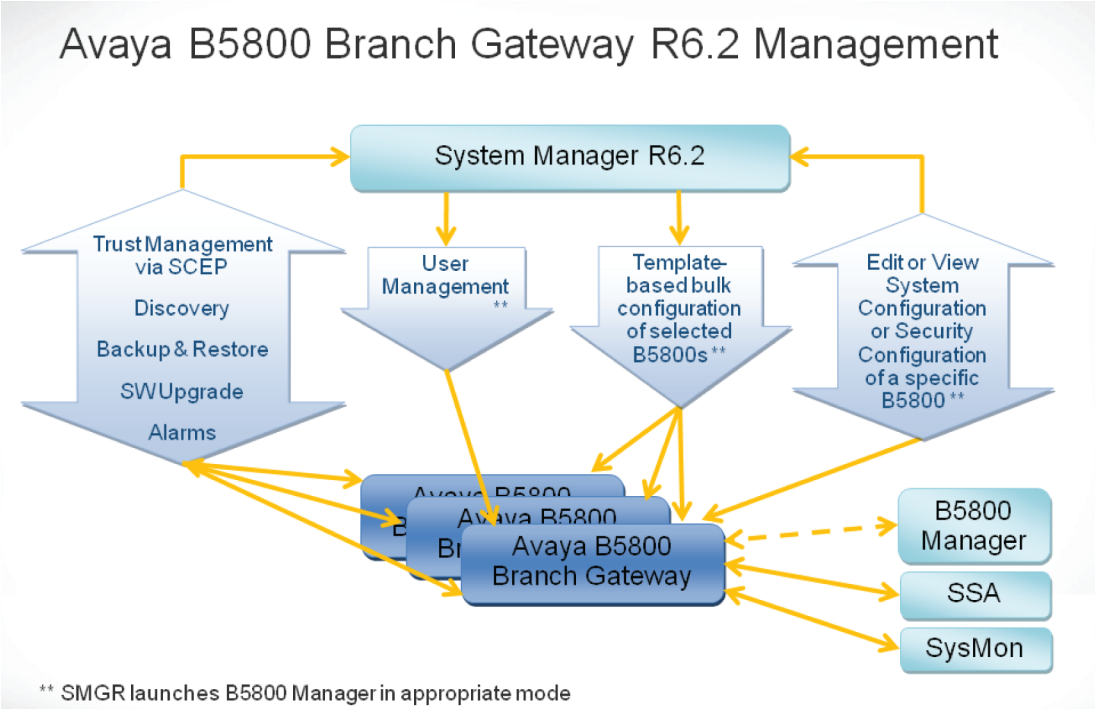
As an alternative to System Manager, you can use IP Office Manager that is directly connected to the B5800 Branch Gateway to configure a branch locally when you need to administer an isolated branch or System Manager is not available. IP Office Manager is an application for viewing and editing a B5800 Branch Gateway system's configuration. It is included in the B5800 Branch Gateway administration software suite. Manager is an off-line editor. It receives a copy of the system's current configuration settings. After changes are made to that copy and the file is saved, Manager automatically sends the file back to the system for those changes to become active.

Avaya Aura® System Manager

Using Avaya Aura® System Manager R6.2, you are able to:

- Upgrade B5800 Branch Gateway systems.
- Add B5800 Branch Gateway devices from the network to System Manager.
- Create B5800 Branch Gateway endpoint templates that are used to create B5800 Branch Gateway users. These templates can be edited, duplicated, or deleted.

- Create B5800 Branch Gateway system configuration templates that can be applied to selected B5800 Branch Gateway systems. These templates are used for initial device provisioning. These templates can be edited, duplicated, or deleted.
- Upload and convert audio files to System Manager to be used in the B5800 Branch Gateway System Configuration Auto Attendant feature.
- Manage B5800 Branch Gateway system configurations. From System Manager, you are able to launch IP Office Manager to view or edit a system configuration. With this feature, you make changes to the B5800 Branch Gateway device through System Manager. You are able to apply the changes immediately or schedule the changes to run at a specified time.
- Manage B5800 Branch Gateway security configuration. From System Manager, you are able to launch IP Office Manager to view or edit a system security configuration. With this feature, you make changes directly to the B5800 Branch Gateway device.
- Create B5800 Branch Gateway user templates. These templates can be edited or deleted.
- Perform a B5800 Branch Gateway backup with the option of storing the backup output in System Manager or creating a local backup where the system stores the backup output on the local storage attached to the B5800 Branch Gateway device.
- Perform a B5800 Branch Gateway restore. This feature allows you to restore:
    - a saved B5800 Branch Gateway system configuration onto a B5800 Branch Gateway from System Manager.
    - a backup of a B5800 Branch Gateway system configuration onto a B5800 Branch Gateway from the device SD card.
    - users from System Manager to the B5800 Branch Gateway.
    - a saved B5800 Branch Gateway system configuration and user from System Manager onto a B5800 Branch Gateway.
- View events and alarms regarding various operations that occur on the B5800 Branch Gateway.



About upgrading B5800 Branch Gateways

With the introduction of centralized management provided by Avaya Aura® System Manager, you are able to upgrade B5800 Branch Gateway firmware and software from System Manager. You are also able to upgrade an individual B5800 Branch Gateway system from IP Office Manager installed on an administration PC that is connected directly to the system. You can perform an upgrade from IP Office Manager using the upgrade wizard or the System SD card.

For more information about these upgrade methods, see the following topics:

- Upgrading the B5800 Branch Gateway using System Manager on page 103
- Using the upgrade wizard on page 217
- System upgrade using the System SD card on page 256

Licensing

B5800 Branch Gateway supports centralized licensing by WebLM where a single license file is generated in Avaya Product Licensing and Delivery System (PLDS) for multiple branches.

Support for individual PLDS license files for each branch (the licensing method provided in B5800 Branch Gateway R6.1) is also an option. WebLM licensing is the recommended method for B5800 Branch Gateway R6.2 and higher. Both licensing methods are described below.

WebLM license management

B5800 Branch Gateway R6.2 supports WebLM licensing in which a single license file is generated in PLDS for multiple branches. This license file contains the host ID of the WebLM server and is managed by the WebLM server. Each B5800 Branch Gateway communicates with the WebLM server to request the required license entitlements. B5800 Branch Gateway uses the Avaya Aura System Manager WebLM server.

Two configuration models are supported:

- WebLM standard licensing model — in this model, one WebLM server is used. This model is used for enterprises where the System Manager WebLM server is able to manage all B5800 Branch Gateway licenses required for the enterprise.
- WebLM enterprise licensing model — in this model, multiple WebLM servers are used. This model is used for enterprises where the licenses required for all branches in the enterprise exceed the System Manager WebLM server capacity. One WebLM server acts as a master WebLM server and hosts the license file from PLDS. The other WebLM servers(s) act as a local WebLM server and host allocation license files from the master WebLM server. Each B5800 Branch Gateway must be configured with the IP address of one of the WebLM servers.

Note:

The expected System Manager WebLM server capacity is about 400 branches on a loaded System Manager. The capacity would be higher on a lightly loaded System Manager. The expected WebLM capacity on a standalone Linux server is about 1,100 branches. Large deployments that exceed the System Manager WebLM capacity require additional standalone WebLM server(s) and configuration of the WebLM servers as master and local in the WebLM enterprise licensing model.

Note:

The correct expiration time of licenses for a B5800 Branch Gateway that uses a local WebLM server is provided on the corresponding master WebLM server. The local WebLM server shows the licenses as having an expiration time of 30 days or less. However, periodically the license expiration time on the local WebLM server is automatically refreshed and extended when the master WebLM server pushes a refreshed Allocation License File to the local WebLM.

For more information about WebLM licensing, see *Administering Avaya WebLM (standalone)* and *Avaya WebLM Administration Guide*.

Separate PLDS license for each branch

In B5800 Branch Gateway R6.1, an individual PLDS license file was required for each branch and installed on each branch directly. A WebLM server was not required. This licensing method is supported in B5800 Branch Gateway R6.2 for branches that cannot be connected via an enterprise WAN to a central WebLM server or for migration of installed B5800 Branch Gateway R6.1 systems. Using the WebLM licensing method is recommended, but does not have to be done as part of an R6.1 to R6.2 upgrade.

For the separate PLDS licensing method, branch licenses are issued and validated against the Feature Key serial number of the System SD card used by that B5800 Branch Gateway. That number is printed after the **FK** prefix on the System SD card and is also shown in the branch system configuration. This means that licenses issued for one branch cannot be used in the configuration of another branch. In the IP Office Manager application, this number appears in the **PLDS Host ID** field on the System page when you select **System > System**.

B5800 Branch Gateway licenses

The B5800 Branch Gateway licenses are described below.

Avaya Branch Gateway System Software license

This license is required for operation of the B5800 Branch Gateway system. This license does not include any implicit entitlements and therefore is not sufficient by itself for branch operation without additional Station and/or SIP Trunk Session licences. One Avaya Branch Gateway System Software license is required.

Native Station licenses

All users on a B5800 Branch Gateway system must be licensed by the addition of Native Station licenses. Native Station licenses are required for all configured users with analog, digital, H.323 or DECT extensions; for users without any extension; and for all users with SIP extensions set as native (or local) (that is, extensions operating in the distributed branch user model).

⚠ Warning:

Unlicensed extensions will display **No License Available** but will be able to make emergency calls, i.e. calls that match B5800 Branch Gateway Dial Emergency short codes.

Embedded Messaging Ports license

This license is required if you are using the B5800 Branch Gateway voicemail options, Embedded Voicemail or Standalone Voice Mail. The Embedded Messaging Ports license is also used to control the number of ports on systems where Avaya Aura Messaging or Modular Messaging over SIP is configured as the central voicemail system and the local Embedded Voicemail provides auto attendant operation. For Embedded Voicemail, up to 6 ports can be licensed. For Standalone Voice Mail, up to 40 ports can be licensed. At least one Embedded Messaging Port license must be purchased to enable this service.

SIP Trunk Sessions license

This license refers to the total number of concurrent sessions allowed on all SIP connections to the B5800 Branch Gateway. The maximum number of SIP trunk sessions is 128. SIP trunks provide the SIP connections between Avaya Aura®Session Manager and B5800 Branch Gateway. SIP trunk sessions are used for connectivity to the telephone company that provides the SIP trunks.

Additional channels licenses

The PRI Universal (PRI-U) trunk card can be used in the B5800 Branch Gateway system. The PRI-U ports can be configured to support E1, E1R2, or T1 line types. Each port supports 8 B channels which do not require a license. Additional B channels beyond these 8 require a license. There are two additional channels licenses that define the number of additional channels (above the default 8):

- **Additional T1 Channels license** — This license is for additional T1 trunks.
- **Additional E1 Channels license** — This license is for additional E1 or E1R2 trunks.

For trunk types on which channels can be set as in service, the licenses are consumed by those channels which are configured as being in service. Manager will block attempts to configure PRI channels as in service if they exceed the 8 per port allowed by default on that card and if there are no Additional T1 Channels or Additional E1 Channels licenses available.

120-day trial license

This license provides a 120-day trial period during which you have access to the features, functions, and capabilities available in B5800 Branch Gateway. After the expiration of the 120-day trial license, the 30-day grace period is activated. At the end of the 30-day grace period, if no other license is installed or available, system administration is blocked, except for administration that fixes the licensing errors.

License modes

The B5800 Branch Gateway system can be in one of three license modes — License Normal Mode, License Error Mode, and License Restricted Mode. The license mode, as well as any license errors, are displayed in IP Office Manager.

License Normal Mode

No license errors are present. The B5800 Branch Gateway can access the WebLM server and obtain the required license entitlements. If the licensing method is used where an individual PLDS license file is required for each branch, a valid license file is installed on the B5800 Branch Gateway with sufficient entitlements.

License Error Mode

One or more license errors are present. The B5800 Branch Gateway initiates a 30–day license grace period during which time the system issues errors and alarms, but continues to provide normal operation as in License Normal Mode. Calls are allowed and/or blocked based on current configuration parameters and configured users can register, regardless of licensing status. The license errors must be fixed either by installing a valid license file with the appropriate licenses or by changing the configuration so that it does not exceed any license capacities.

License Restricted Mode

One or more license errors are present and the 30–day license grace period has expired. B5800 Branch Gateway prevents any administrative changes except those that fix the licensing

errors. While administration is restricted, dynamic system operation (such as making calls) continues based on the current configuration parameters, regardless of licensing status.

System components

The B5800 Branch Gateway system is comprised of the following hardware components.

- **B5800 Branch Gateway control unit** — B5800 Branch Gateway is supported on the IP500v2 platform or on the B5800 Branch Gateway hardware platform which is based on IP500v2. The B5800 Branch Gateway control unit stores the system configuration and performs the routing and switching for telephone calls and data traffic. It includes 4 slots for optional base cards to support trunk and phone extension ports. The slots are numbered 1 to 4 from left to right. They can be used in any order; however, if the capacity for a particular type of card is exceeded, the card in the right-most slot will be disabled.
- **B5800 Branch Gateway System SD card** — The B5800 Branch Gateway System SD card is a specific Avaya SD card that is required. It determines the system operation as B5800 Branch Gateway. It is uniquely numbered and has a serial number that must be used as the Host ID in the PLDS license file if the B5800 Branch Gateway is operating with an individual license file and not with WebLM licensing. The B5800 Branch Gateway System SD card also provides Embedded Voicemail support and storage for system software files. The card fits into a slot in the rear of the control unit.
- **Base cards** — The control unit has slots for up to 4 base cards. The base cards are used to add analog extension ports, digital extension ports, and voice compression channels. Each base card includes an integral front panel with ports for cable connections. The following base cards are supported:
  - **Digital station base card** — This card provides 8 digital station (DS) ports for the connection of Avaya digital phones other than IP phones. The card can be fitted with a trunk daughter card which uses the base card ports for trunk connection. A maximum of 3 digital station base cards are allowed per control unit.
  - **Analog phone base card** — This card is available in two variants, supporting either 2 or 8 analog phone ports. The card can be fitted with a trunk daughter card which uses the base card ports for trunk connection. A maximum of 4 analog phone base cards are allowed per control unit. The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors. If fitted with an analog trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12.
  - **VCM base card** — This card is available in variants supporting either 32 or 64 Voice Compression Channels (VCM) for use with VoIP calls. A maximum of 2 VCM base cards are allowed per control unit. The card can be fitted with a trunk daughter card which uses the base card ports for trunk connection.
  - **4–port expansion base card** — This card adds an additional 4 expansion ports for external expansion modules. The card is supplied with four 2m yellow interconnect

cables. This card does not accept any trunk daughter cards. A maximum of 1 4–port expansion base card is allowed per control unit (right-hand slot 4 only). See External expansion modules on page 22 for a list of the supported external expansion modules.

- **BRI combination card** — This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 2 BRI trunk ports (9-10, 4 channels). The card also includes 10 VCM channels. This card has a pre-installed BRI trunk daughter card. A maximum of 2 BRI combination cards of any type are allowed per control unit.
- **ATM combination card** — This card provides 6 digital station ports (1-6), 2 analog extension ports (7-8) and 4 analog trunk ports (9-12). The card also includes 10 VCM channels. This card has a pre-installed analog trunk daughter card. A maximum of 2 ATM combination cards of any type are allowed per control unit. The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors. If fitted with an analog trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12.
- **TCM 8 card** — This card provides 8 digital station ports (1-8).

• **Trunk daughter cards** — Most base cards can be fitted with a trunk daughter card to support the connection of trunks to the base card. The following trunk daughter cards are supported:

- **Analog trunk card** — This card allows the base card to support 4 analog loop-start trunks. The analog phone ports do not include a ringing capacitor. Where this is a requirement, connection should be via a Master socket containing ringing capacitors. If fitted with an analog trunk daughter card, during power failure phone port 8 is connected to analog trunk port 12. A maximum of 4 analog trunk cards are allowed per control unit.
- **BRI trunk card** — This card allows the base card to support up to 4 BRI trunk connections, each trunk providing 2B+D digital channels. The card is available in 2 port (4 channels) and 4 port (8 channels) variants. A maximum of 4 BRI trunk cards are allowed per control unit. For S-Bus connection, the card can be switched from To trunk mode to So mode. This mode requires additional terminating resistors and an ISDN crossover cable connection.
- **PRI trunk card** — This card allows the base card to support up to 2 PRI trunk connections. The card is available in single and dual port variants. The card can be configured for E1 PRI, T1 robbed bit, T1 PRI or E1R2 PRI trunks. A maximum of 4 PRI trunk cards are allowed per control unit. The B5800 Branch Gateway system supports 8 unlicensed B-channels on each IP500 PRI-U port fitted. Additional B-channels, up to the capacity of ports installed and PRI mode selected require Universal PRI (Additional Channels) licenses added to the configuration. These additional channels consume the licenses based on which additional channels are configured as in-service from port 9 of slot 1 upwards. D-channels are not affected by licensing.

• **Combination cards** — Combination cards are pre-paired base and trunk daughter cards. They provide 6 digital station ports, 2 analog phone ports, 10 VCM channels and either

4 analog trunk ports or 4 BRI channels (2 ports). The trunk daughter card cannot be removed or replaced with another type of trunk daughter card.

- **External expansion modules** — External expansion modules are used to add additional analog and digital ports. If the control unit is fitted with a 4–port expansion base card, then up to 12 external expansion modules are supported. The following external expansion modules are supported:
  - **Analog trunk module** — This module rovides an additional 16 analog ports for connection of analog trunks. It supports both loop-start and ground-start trunks.
  - **BRI So8 module** — This module provides 8 ETSI BRI-So ports for the connection of ISDN devices. This module is not intended to support BRI trunks.
  - **Digital station module** — This module provides, depending on variant, an additional 16 or 30 DS ports for supported Avaya digital phones.
  - **Phone module** — This module provides, depending on variant, an additional 16 or 30 phone ports for analog phones.
- **Power supplies** — The control unit has an internal power supply unit. Each external expansion module is supplied with an external power supply unit. Additional power supply units may also be required for IP phones and some phone add-ons.
- **Power cords** — Depending on the locale, different power cords need to be ordered for each control unit, external expansion module, and any phones or devices using external power supply units.
- **Mounting kits** — The control unit can be used free-standing, with external expansion modules stacked above it. With optional rack mounting kits, the control unit and external expansion modules can also be rack mounted. Alternatively, with an optional wall mounting kit the control unit can be wall mounted. However, the control unit cannot support any external expansion modules when wall mounted.
- **Surge protectors and barrier boxes** — Where the installation includes extensions in other buildings, additional protective equipment is required. This equipment may also be required in areas where the lightning risk is high.
- **Phones** — B5800 Branch Gateway systems support a variety of Avaya digital and IP phones plus analog phones.
- **Application DVDs** — The B5800 Branch Gateway applications can be ordered on a number of DVDs. In addition they can be downloaded from the B5800 Branch Gateway section of the Avaya support web site (http://support.avaya.com).

Supported telephones

Telephone	Native extensions (local extensions operating in the distributed branch user model)
Analog	✔
1120E SIP	✔
1140E SIP	✔
1220 SIP	✔
1230 SIP	✔
1403 digital	✔
1408 digital	✔
1416 digital	✔
1603	✔
1603SW	✔
1608	✔
1616	✔
1603SW-I	✔
1608-I	✔
1616-I	✔
BM32 (DSS)	✔[1]
2402D	✔
2410D	✔
2420	✔
3616 wireless	✔
3620 wireless	✔
3626 wireless	✔
3641 wireless	✔
3645 wireless	✔
3720 DECT R4	✔
3725 DECT R4	✔

Telephone	Native extensions (local extensions operating in the distributed branch user model)
3740 DECT R4	✔
3749 DECT R4	✔
3810 digital wireless	✔
4601	✔
4602IP	✔
4602SW	✔
4610IP	✔
4610SW	✔
4621	✔
4625	✔
5402	✔
5410	✔
5420	✔
EU24 (DSS)	✔[1]
5601	✔
5602IP	✔
5602SW	✔
5610IP	✔
5610SW	✔
5620	✔
5621	✔
EU24 BL (DSS)	✔[1]
9504 digital	✔
9508 digital	✔
9608	✔[2]
9611G	✔[2]
9621G	✔[2]
9641G	✔[2]
9620L	✔[2]
9620C	✔[2]

Telephone	Native extensions (local extensions operating in the distributed branch user model)
9630G	✔[2]
9640	✔[2]
9640G	✔[2]
9650	✔[2]
9650C	✔[2]
SBM24	✔[1]
Avaya 1010/1020/1030/1040 video conferencing units	✔
B149 conference phone	✔
B159 conference phone	✔
B179 conference phone	✔
BM12	✔[1]
BCM TDM sets: • DECT handsets 4xxx/7xxx series • T7316E • T7316 • T7406E • T7406 • T7208 • T7100 • T7000 • M7310 • M7310N • M7310+BLF • M7324 • M7324N • M7208 • M7208N • M7100 • M7100N	✔

Telephone	Native extensions (local extensions operating in the distributed branch user model)
• Audio conference unit • T24 KIM (Key Indicator Module for T7316)	
DevConnect–approved 3rd-party SIP audio and video endpoints	✔

[1] When connected to their respective telephones.

[2] Supported when running H.323 firmware; *not* supported when running SIP firmware.

Software applications

The B5800 Branch Gateway software applications are provided on DVDs.

- **User applications** — The following applications are supported for use by native users on a B5800 Branch Gateway system.
  - **Embedded Voicemail**: supports basic voicemail mailbox operation, simple auto-attendants and hunt group announcements. It is provided on the Avaya SD card. Embedded Voicemail on a B5800 Branch Gateway system provides 6 ports. This voicemail option requires a license. See Licensing on page 16 for more information.
  - **Standalone Voicemail**: provides additional port capacity (40 ports) on a Linux server. You must have a Linux server installed to use this option. This voicemail option requires a license. See Licensing on page 16 for more information.
  - **SoftConsole**: is intended for telephone system operators or receptionists. It displays details of calls and allows them to quickly see the status of the callers required destination and transfer the call. The SoftConsole user is able to access a range of details about the status of users and groups on the B5800 Branch Gateway system. Up to 4 simultaneous SoftConsole users can be configured. This application does not require a license.
- **Installer/maintainer applications** — The following B5800 Branch Gateway applications are used to program and maintain a B5800 Branch Gateway system. These applications do not require a license.
  - **Manager**: a configuration application used to access all parts of the B5800 Branch Gateway configuration. Different levels of access can be defined to control which parts of the configuration the Manager user can view and alter. Manager is also used to upgrade the software files used by a B5800 Branch Gateway system.

- **System Status**: a monitoring application used to inspect the current status of B5800 Branch Gateway lines and extensions and to view records of recent alarms and events. It runs as a Java application.
- **System Monitor**: shows a trace of all activity on the B5800 Branch Gateway system in detail. Interpretation of System Monitor traces requires a high-level of data and telephony protocol knowledge. B5800 Branch Gateway installers and maintainers must run System Monitor when Avaya requests copies of System Monitor traces to resolve support issues.
- **SNMP MIBs**: Not an application as such, the SNMP MIB files can be used by 3rd-party SNMP applications to monitor the B5800 Branch Gateway system.

Supported country locales

When a new or defaulted system's configuration is first opened in Manager, the value set in the **Locale** field (**System** > **System** > **Locale**) should always be checked and changed if necessary. The system's locale sets factors such as the default ringing patterns and caller display settings. The locale also controls the language that a voicemail server will use for prompts.

The following table indicates locale settings supported for different functions. Note that this does not necessarily indicate support, availability or approval for B5800 Branch Gateway within that country.

Locale	Language	Telephony	Phone Display	Applications		EVM and SVM*
				Manager	Soft Console	
Argentina	**Latin Spanish**	✓	✓	✓	✓	✓
Australia	**UK English**	✓	✓	✓	✓	✓
Belgium	**Dutch**	✓	✓	✓	✓	✓
Belgium	**French**	✓	✓	✓	✓	✓
Brazil	**Brazilian**	✓	✓	✓	✓	✓
Canada	**Canadian French**	✓	✓	-	-	✓
Chile	**Latin Spanish**	✓	✓	✓	✓	✓
China	**Mandarin**	✓	-	-	✓	✓
Colombia	**Latin Spanish**	✓	✓	✓	✓	✓

Locale	Language	Telephony	Phone Display	Applications		EVM and SVM*
				Manager	Soft Console	
Denmark	**Danish**	✓	✓	-	✓	✓
Finland	**Suomi**	✓	✓	-	✓	✓
France	**French**	✓	✓	✓	✓	✓
Germany	**German**	✓	✓	✓	✓	✓
Greece	**Greek**	✓	-	-	-	SVM only
Hong Kong	**Cantonese**	✓	-	-	-	-
Hungary	**Hungarian**	✓	-	-	-	SVM only
Iceland	**Icelandic**	✓	-	-	-	-
India	**UK English**	✓	-	✓	✓	✓
Italy	**Italian**	✓	✓	✓	✓	✓
Korea	**Korean**	✓	-	-	✓	✓
Mexico	**Latin Spanish**	✓	✓	✓	✓	✓
Netherlands	**Dutch**	✓	✓	✓	✓	✓
New Zealand	**UK English**	✓	✓	✓	✓	✓
Norway	**Norwegian**	✓	✓	-	✓	✓
Peru	**Latin Spanish**	✓	✓	✓	✓	✓
Poland	**Polish**	✓	-			SVM only

* **EVM** is Embedded Voicemail. **SVM** is Standalone Voice Mail.

Note:

Hungarian, Polish, and Greek are not supported by Embedded Voicemail, but they are supported by Standalone Voice Mail.

- **Locale:** The country represented by the locale.
- **Language:** The voicemail prompt language used for that locale.
- **Telephony:** The B5800 Branch Gateway provides default telephony settings matching the normal expected defaults for the locale.
- **Phone Display:** Indicates that display messages from the B5800 Branch Gateway to Avaya phones can be sent using the appropriate language for that locale. Note that the user locale can be used to override the system locale for these messages. Note also that some phones support their own language selection options for menus displayed by the phone's own software.

- **Manager:** Indicates that the IP Office Manager application can run in the specific locale language. Manager uses the best match it has (French, German, Brazilian, Dutch, Italian, Mexican Spanish, Russian, or US English) for the regional location setting of the PC on which it is running, otherwise it defaults to UK English. If required the language used within the Manager screens can be overridden.
- **Embedded Voicemail:** Indicates that the locale is recognized by Embedded Voicemail and appropriate language prompts are then used. If an unsupported locale is used, Embedded Voicemail will attempt the best match using the first two characters of the locale. The system locale can be overridden by setting a different user locale.
- **Standalone Voice Mail:** Indicates that the locale is recognized by Standalone Voice Mail and appropriate language prompts are then used. If an unsupported locale is used, Standalone Voice Mail will attempt the best match using the first two characters of the locale. The system locale can be overridden by setting a different user locale.

New in this release

Avaya B5800 Branch Gateway Release 6.2 provides the following new features:

- **Centralized management provided by Avaya Aura® System Manager** — provides centralized management for single provisioning of native (local) users in distributed branch deployments. System Manager replaces the Network Management applications that were used for centralized management in B5800 Branch Gateway R6.1. See Management on page 14 for more information.
- **Licensing** — support for centralized licensing by WebLM server. A single license file is generated in PLDS for multiple branches. License entitlements are shared among multiple B5800 Branch Gateways.
- **Heritage-Nortel branch migration to B5800 Branch Gateway** — support for Norstar and BCM digital T&M Series phones and 11xx/12xx phones running SIP 4.3. Support for B5800 Branch Gateway with CS 1000 R7.5 core in distributed branch deployments.

  Note:

  Integration of B5800 Branch Gateway with Communication Server 1000 is provided in a separate document. See *Implementing the Avaya B5800 Branch Gateway for a Communication Server 1000 Configuration*.

- **Voicemail** — support for Avaya Aura Messaging, Standalone Voice Mail, and CallPilot.

  Avaya Aura Messaging or CallPilot can be configured as the central voicemail system. With this option, you are still able to use Embedded Voicemail or Standalone Voice Mail at each branch to provide auto-attendant operation and announcements for waiting calls.

Note:

Release 6.2 does not support VMPro.

Standalone Voice Mail provides additional port capacity (40 ports) provided on a Linux server. You must have a Linux server installed to use this option.

- **Endpoints** — support for the following new native phones (operating in distributed branch user model): 3740/3749 DECT R4; 3810 (digital wireless); 9504, 9508 (digital); 9611G; B149, B159 and B179 conference phones (former Konftel); 1120E, 1140E, 1220, 1230 (SIP); The following BCM digital phones: DECT handsets 4xxx/7xxx series, T7316E, T7316, T7406E, T7406, T7208, T7100, T7000, M7310, M7310N, M7310+BLF, M7324, M7324N, M7208, M7208N, M7100, M7100N, ACU (audio conference unit)
- **Contact Center** — support for Contact Center service interoperability. IP Agent or Avaya one-X® Agent in branch in Telecommuter mode with CC-Elite; calls transferred from B5800 Branch Gateway to contact center; B5800 Branch Gateway handling VoicePortal transfer with UUI in SIP.
- **Park and Page** — support for the Park and Page feature when the system voicemail type is configured as Embedded Voicemail or Standalone Voice Mail. Park and Page is also supported on systems where Avaya Aura Messaging, Modular Messaging over SIP, or CallPilot is configured as the central voicemail system and the local Embedded Voicemail provides auto attendant operation. The Park and Page feature allows a call to be parked while a page is made to a hunt group or extension.
- **Additional new features**:
  - **Enable voicemail instructions using DTMF** — support for enhanced voicemail continuity over the PSTN. Available for Avaya Aura Messaging or Modular Messaging over SIP central voicemail systems, this feature facilitates getting the call to the specific mailbox rather than to the general prompt. When a PSTN number is configured, B5800 Branch Gateway will send voicemail calls to that PSTN number when Avaya Aura Session Manager is not available.

    Note:

    In Release 6.2, this feature is not available for CallPilot.

  - **Export user tool** — for an R6.1 to R6.2 upgrade, support for exporting all users or selected users from a loaded configuration to an XML file that is then imported in Avaya Aura System Manager. During a B5800 Branch Gateway R6.1 to R6.2 upgrade, users are not automatically created in System Manager. After an R6.1 to R6.2 upgrade, B5800 Branch Gateway users are exported to a file and then the file is imported to System Manager.
  - **Music on Hold** — administrator is able to change the Music on Hold. Supported audio file formats are PCM or WAW.

Related resources

Related documents

Ensure that you have read this manual before starting the installation. Also read the installation documentation for any other equipment and applications being installed as part of the B5800 Branch Gateway system.

Documents you may need to consult are as follows:

- Administering Avaya Aura® System Manager
- Administering Avaya Aura® Session Manager, document number 03-603324
- Avaya IP Office Manager Release 6.2, document number 15-601011
- Implementing Embedded Voicemail for B5800 Branch Gateway Release 6.2, document number 18-604098.
- Implementing Standalone Voice Mail for B5800 Branch Gateway Release 6.2, document number 18-604088.
- Avaya B5800 Branch Gateway Solution Overview Release 6.2, document number 18-603903
- Avaya WebLM Administration Guide
- Administering Avaya WebLM (standalone)

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit http://www.youtube.com/AvayaMentor and do one of the following:

- Enter a key word or key words in the Search channel to search for a specific product or topic.
- Click the name of a playlist to scroll through the posted videos.

Training

Avaya University provides a wide range of training courses for B5800 Branch Gateway and its associated applications. This includes courses necessary for B5800 Branch Gateway resellers

to become Avaya Authorized Channel Partners and for individuals to achieve B5800 Branch Gateway certification.

Details of courses can be found on the Avaya University web site (http://www.avaya-learning.com). The site can be used to check course availability and to book courses. It also includes on-line courses and on-line course assessments. The site requires users to setup a user name and password in order to track their personal training record.

For a list of recommended courses available for the B5800 Branch Gateway, see Recommended courses for Avaya B5800 Branch Gateway training on page 303.

Web sites

Information to support B5800 Branch Gateway can be found on a number of web sites.

- Avaya (http://www.avaya.com)

  The official web site for Avaya. The front page also provides access to individual Avaya web sites for different countries.

- Avaya Enterprise Portal (http://partner.avaya.com)

  This is the official web site for all Avaya Business Partners. The site requires registration for a user name and password. Once accessed, the site portal can be individually customized for what products and information types you wish to see and to be notified about by email.

- Avaya Support (http://support.avaya.com)

  Contains documentation and other support materials for Avaya products.

- Avaya University (http://www.avaya-learning.com)

  This site provides access to the full range of Avaya training courses. That includes both on-line courses, course assessments and access to details of classroom based courses. The site requires users to register in order to provide the user with access to details of their training record.

- Avaya Community (http://www.aucommunity.com)

  This is the official discussion forum for Avaya product users. However it does not include any separate area for discussion of B5800 Branch Gateway issues.

Revision history

Issue	Date	Summary of changes
2	07/2012	• The name of the B5800 Branch Gateway security certificate cannot contain spaces. This is explained in a note in the appropriate places. • The order of the steps in the “Configuration checklist” have been changed. The step to add the B5800 Branch Gateway to System Manager has been moved to after you generate a certificate and run the Initial Installation Utility. • Two additional fields may need to be edited in the xml file used to export users during an R6.1 to R6.2 upgrade. Those fields have been added to the procedure “Editing the xml file containing the users.”
3	10/2012	Modifications have been made to the following procedures: • “Generating a certificate on System Manager” (Additional steps have been added to the procedure for clarity.) • “Using the Initial Installation Utility” (It is recommended to select LAN1 to configure the WAN interface.) • “Configuring the B5800 Branch Gateway for certificates” (This procedure replaces “Manually loading the certificate to the B5800 Branch Gateway.) • “Adding distributed users to System Manager” (Distributed H.323 users and SIP users do not require different configuration when being added to System Manager.)

Chapter 2: Planning

Before you begin installing and configuring the B5800 Branch Gateway system, you should already have determined the implementation issues listed in the table below.

You have determined...	See	✔
The dial plan you are configuring for the system and each branch.	Dial plan considerations on page 36	
The B5800 Branch Gateway licenses required for this installation.	Licensing on page 16	
How you are going to route outgoing PSTN calls.	Branch PSTN call routing considerations on page 38	
The voicemail solution you are going to deploy.	Voicemail considerations on page 37	
VoIP requirements.	Network assessment for VoIP requirements on page 39	

Prerequisites

Depending upon the deployment, the following applications and servers must be installed and configured before the B5800 Branch Gateway system is installed.

- If you are going to connect the B5800 Branch Gateway to an enterprise over the WAN, Avaya Aura® Session Manager R6.1 or R6.2 must be installed and configured at the headquarters location.
- If you are going to centrally manage the B5800 Branch Gateways, Avaya Aura® System Manager R6.2 must be installed and configured at the headquarters location.
- If you are going to use centralized licensing by WebLM, an Avaya Aura® System Manager WebLM server or a standalone WebLM server must be installed and configured. The WebLM server can be located at the headquarters location or anywhere in the network as long as the B5800 Branch Gateways can access it on the network.
- A stand-alone Secure Access Link (SAL) Gateway, R2.0 or higher, must be deployed.

Note:

System Platform's virtual SAL gateway is not supported.

Dial plan considerations

A uniform dial plan greatly simplifies configuration, management and phone calls within the network branch sites. For example, if each branch has similar roles such as reception, manager and warehouse - using the same extension number for each role and a unique prefix for each branch allows calls between sites with little need for directory lookups. It also means a standard configuration can be used at branches; simplifying installation, user training and maintenance.

For our examples we have used the following dial plan for each branch site:

- **3-digit branch prefixes beginning with 8** — A 3-digit branch prefix in the range 800 to 899. This allows us up to 100 branches yet keeps call routing simple. Any dialing at a branch that being with an 8 can be assumed to be a call to a branch number and can be routed to the Avaya Aura® Session Manager for routing to the correct branch.
- **3-digit extension numbers beginning with 2** — 3-digit extension numbers for all native extensions and hunt groups starting from 200. This is the default numbering used by B5800 Branch Gateway.

Dial plan example

To describe a dial plan example, we have created Acme Travel, a travel agency with a growing number of branches. Each branch follows the same pattern, with extensions for a branch manager and a small team of travel consultants in a sales group.

Given the nature of the business, branch users need to make national and international calls. The company has taken advantage of a bulk call contracts from it headquarters site so wants such calls routed via the headquarters site wherever possible. In addition, the branch staff want to keep their branch phone numbers.

- 3-digit branch numbers beginning with 8, ie. 800 to 899.
- 3-digit native extension numbers beginning with 2, ie. 200 to 299.
- Dial 9 prefix for outgoing PSTN calls.
- National and international calls allowed but routed via the headquarters site's PSTN trunks.
- Where a national call matches a branch location, it should be routed to the PSTN via that branch.
- Local calls allowed from each branch using its own PSTN trunks.

- Modular Messaging at the headquarters site provides voicemail services to all employees.
- The LAN on each branch has a unique IP address, 192.168.42.1, 192.168.44.1 and so on.
- National calls are made via the branch's PSTN trunks when the branch data connection to the headquarters site is not available or at maximum capacity.

This example assumes that all the branches were initially setup with the default North American locale. For B5800 Branch Gateway that means that a dial 9 prefix is used for external calls. For calls in other locales or between branches in different locals, the example will need to be adjusted to ensure that the resulting number received at the remote branch will be routed to an external PSTN trunk and is suitable for external dialing.

Voicemail considerations

The B5800 Branch Gateway system uses its Embedded Voicemail by default. However, a number of other voicemail options are supported.

- **Embedded Voicemail** — Embedded Voicemail uses the system SD card in the B5800 Branch Gateway system control unit for storage of prompts and messages. Embedded Voicemail supports mailboxes for all local extension numbers, announcements to waiting callers, and auto attendants (up to 40) for external calls. Its capacity is limited to 15 hours of recorded messages, prompts and announcements. Embedded Messaging Port licenses must be purchased with sufficient quantity to support the configured number of ports.
- **Standalone Voice Mail** — Standalone Voice Mail provides the same features as Embedded Voicemail but with additional port capacity provided on a Linux server. You must have a Linux server installed to use this option. When you select this option, you must enter the IP address of the Linux server where Standalone Voice Mail is installed. This option provides a maximum capacity of 40 ports while the Embedded Voicemail option provides a maximum capacity of 6 ports. Embedded Messaging Port licenses must be purchased with sufficient quantity to support the configured number of ports.
- **Avaya Aura Messaging** — The B5800 Branch Gateway system can be configured to use Avaya Aura Messaging as its voicemail server when Session Manager is used as the core SIP router. See Configuring B5800 Branch Gateway to use Avaya Aura Messaging for voicemail on page 176 for more information. When Avaya Aura Messaging is used as the central voicemail system, at each branch you have the option to still use the local Embedded Voicemail for auto attendant operation and for announcements to waiting calls. Note that for this configuration, Embedded Voicemail licenses are required.
- **Modular Messaging over SIP** — The B5800 Branch Gateway system can be configured to use Modular Messaging over SIP as its voicemail server when Session Manager is used as the core SIP router. See Configuring B5800 Branch Gateway to use Modular Messaging over SIP for voicemail on page 178 for more information. When Modular Messaging over SIP is used as the central voicemail system, at each branch you have the option to still use the local Embedded Voicemail for auto attendant operation and for

announcements to waiting calls. Note that for this configuration, Embedded Voicemail licenses are required.

For more information about licensing, see Licensing on page 16.

The Park and Page feature is supported when the system voicemail type is configured as Embedded Voicemail or Standalone Voice Mail. Park and Page is also supported on systems where Avaya Aura Messaging or Modular Messaging over SIP is configured as the central voicemail system and the local Embedded Voicemail provides auto attendant operation. The Park and Page feature allows a call to be parked while a page is made to a hunt group or extension. See Configuring Embedded Voicemail on page 173 for more information.

Branch PSTN call routing considerations

Each B5800 Branch Gateway system can support its own external PSTN trunks. When deployed in an Avaya Aura® network, you have considerable flexibility over where outgoing PSTN calls should emerge from the network and similarly where incoming calls should be routed.

For examples of some of the options available, see Branch PSTN call routing examples on page 289. The examples demonstrate the following options:

- Centralized call control on page 289 — External calls at a branch site can be rerouted to be dialed out at another site. This can be done for reasons of call cost and call control. For example, the central site may have a bulk call tariff for national and international calls that would benefit all branches.
- Branch PSTN Override on page 292 — Having configured the branch to send outgoing external calls to the Avaya Aura® Session Manager for onward routing, there may be cases where a specific number should still be routed via the branches own PSTN trunks.
- PSTN Fallback on page 294 — The B5800 Branch Gateway can be configured to allow some calls that would normally use the Avaya Aura® Session Manager line to be routed via the PSTN when the Avaya Aura® Session Manager line is not available.

The various methods used in the these examples can be combined to match the customer's needs. However the main aim should be as follows:

- To keep the branch configuration as generic as possible, i.e. to use the same PSTN call control in all branch configurations. This simplifies maintenance of multiple branches.
- To centralize as much of the PSTN call control in the Avaya Aura® Session Manager as possible. Again this simplifies maintenance and control.

Network assessment for VoIP requirements

B5800 Branch Gateway is a converged telephony system, that is, it combines aspects of traditional PABX telephone systems and IP data and telephony systems. This works at various levels.

- Individual phone users can control the operation of their phone through applications running on their PC.
- Data traffic can be routed from the LAN interface to a telephony trunk interface, for example a dial-up ISP connection.
- Voice traffic can be routed across internal and external data links. This option is referred to as voice over IP (VoIP).

The VoIP mode of operation can include IP trunks between customer systems and/or SIP telephones for users. In either case the following factors must be considered:

- The B5800 Branch Gateway control unit must be fitted with voice compression channels. These channels are used whenever an IP device (trunk or extension) needs to communicate with a non-IP device (trunk or extension) or a device that uses a different codec.
- A network assessment is a mandatory requirement for all systems using VoIP. For support issues with VoIP, Avaya may request access to the network assessment results and may refuse support if those are not available or satisfactory.

A network assessment includes a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet both current and planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies, and setting voice quality objectives.
- The assessment should leave you confident that the implemented network will have the capacity for the foreseen data and voice traffic, and can support SIP, DHCP, TFTP and jitter buffers in SIP applications.
- An outline of the expected network assessment targets is:

Test	Minimum Assessment Target
Latency	Less than 150ms
Packet Loss	Less than 3%
Duration	Monitor statistics once every minute for a full week

Chapter 3: Installation requirements

This chapter provides information about power supplies, cables, grounding and environmental and space requirements for installing the B5800 Branch Gateway control unit and external expansion modules. The B5800 Branch Gateway control unit can be mounted on the wall if no external expansion units are included in the installation. If the installation includes external expansion modules, the control unit and external expansion modules can be mounted into a standard 19-inch rack system.

Power supply backup (UPS)

The use of an Uninterrupted Power Supply (UPS) with any telephone system is strongly recommended. Even at sites that rarely lose electrical power, that power may occasionally have to be switched off for maintenance of other equipment. In addition, most UPSs also provide an element of power conditioning, reducing spikes and surges.

The capacity of UPS systems and the total equipment load the UPS is expected to support are usually quoted in VA. Where equipment load is quoted in Watts, multiply by 1.4 to get the VA load.

The calculation of how much UPS capacity is required depends on several choices.

- **What equipment to place on the UPS?** Remember to include server PCs such as the voicemail. It is recommended that the total load on a new UPS is never greater than 75% capacity, thus allowing for future equipment.
- **How many minutes of UPS support is required?** Actual UPS runtime is variable, it depends on what percentage of the UPSs capacity the total equipment load represents. For example, a 1000VA capacity UPS may only support a 1000VA (100%) load for 5 minutes. This relationship is not linear, the same UPS would support a 500VA (50%) load for 16 minutes. Therefore the lower the percentage of capacity used, the increasingly longer the UPS runtime, typically up to 8 hours maximum. Remember also that for most UPS's the ratio of discharge to full recharge time is 1:10.
- **How many output sockets does the UPS provide?** Multiple UPS units may be required to ensure that every item of supported equipment has its own supply socket.

The web site http://www.avayaups.com provides a calculator into which you can enter the equipment you want supported on a UPS. It will then display various UPS options. The site uses VA values for typical B5800 Branch Gateway systems. However, if more specific values are required for a particular system, the table below can be used to enter values.

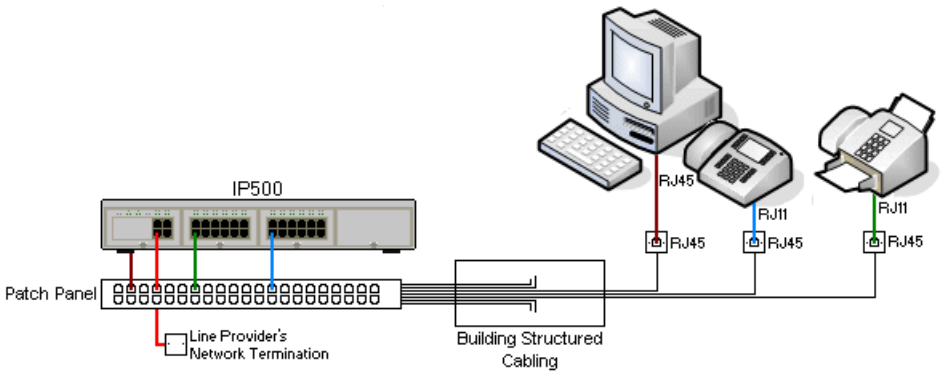
Typical B5800 Branch Gateway System	VA
B5800 Branch Gateway system	230
Individual Equipment	**VA**
Analog 16 module	88
Digital Station 16 module	34
Digital Station 30 module	42
WAN3 module	17
So8 module	34

The 1151D2 power supply unit for Avaya H.323 IP phones includes a backup battery. This typically provides 15 minutes backup at maximum load (20 Watts) and up to 8 hours at light load (2 Watts).

Cables

The B5800 Branch Gateway system is designed primarily for use within an RJ45 structured cabling system using CAT3 unshielded twisted-pair (UTP) cabling and RJ45 sockets.

A structured cabling system is one where cables are run from a central RJ45 patch panel in the communications/data room to individual RJ45 sockets at user locations. All wires in each cable between the patch panel and the desk socket are connected straight through. This arrangement allows devices connected at the patch panel to be swapped to match the type of device that needs to be connected at the user socket. For example, making one user socket a phone port and another user socket a computer LAN port, without requiring any rewiring of the cables between the patch panel and the user location.



- **Traditional IDC punchdown wiring installations** — Where necessary, the far end RJ45 plug can be stripped from B5800 Branch Gateway cables and wired into traditional wiring

systems using punch-block connectors. This type of installation should be performed by an experienced wiring technician.

- **Trunk connections** — The majority of B5800 Branch Gateway trunk ports use RJ45 connectors for acceptance of an RJ45-to-RJ45 cable. However, connection at the line provider's end may require use of a different plug type in order to match the line providers equipment.
- **RJ11 phone connectors** — Many phones use RJ11 sockets and are supplied with RJ11-to-RJ11 cables. RJ11 plugs can be inserted into RJ45 sockets and in many case the connection will work. However this is not recommended or supported as the connection lock is not truly positive and may become disconnected. An RJ45-to-RJ11 cable is available for these connections.

Standard B5800 Branch Gateway cables

The following are Avaya standard cables available for use with B5800 Branch Gateway systems. The maximum length is applicable if the standard Avaya cable is replaced with an alternate cable.

Cable	Description	Standard Length	Maximum Length
9-way DTE cable	Connects to control unit RS232 DTE port. 9-way D-type plug to 9-way D-type socket.	2m/6'6"	2m/6'6"
Structured cabling DS line cable	Connects from RJ45 sockets to RJ11 socketed DS and analog phones.	4m/13'2"	–
BRI/PRI trunk cable	Connects BRI/PRI trunk ports to the line provider's network termination point. RJ45 to RJ45. Red.	3m/9'10"	–
Expansion interconnect cable	Connects the control unit to expansion modules (except WAN3 modules). RJ45 to RJ45. Blue.	1m/3'3"	1m/3'3"
LAN cable	Connects from B5800 Branch Gateway LAN ports toB5800 Branch Gateway devices. RJ45 to RJ45. Grey.	3m/9'10"	100m/328'
V.24 WAN cable	37-way D-type plug to 25-way D-type plug.	3m/9'10"	5m/16'5"
V.35 WAN cable	37-way D-type plug to 34-way MRAC plug.	3m/9'10"	5m/16'5"
X.21 WAN cable	37-way D-type plug to 15-way D-type plug.	3m/9'10"	5m/16'5"

Grounding

Use of ground connections reduces the likelihood of problems in most telephony and data systems. This is especially important in buildings where multiple items of equipment are interconnected using long cable runs, for example phone and data networks.

All control units and external expansion modules must be connected to a functional ground. Where the unit is connected to a power outlet using a power cord with an earth lead, the power outlet must be connected to a protective earth.

In some cases, such as ground start trunks, in addition to being a protective measure this is a functional requirement for the equipment to operate. In other cases it may be a locale regulatory requirement and or a necessary protective step, for example areas of high lightning risk.

For more information about grounding including the location of the ground points on the control unit and external expansion modules, see Grounding on page 71.

Wall and rack mounting

The B5800 Branch Gateway control unit is designed to be freestanding. When external expansion modules are used, the control unit and expansion modules are intended to be stacked. With optional mounting kits, the system can be wall or rack mounted. See Wall mounting on page 65 and Rack mounting on page 67 for more information.

Voice compression channels

Calls to and from IP devices can require conversion to the audio codec format being used by the IP device. For B5800 Branch Gateway systems this conversion is done by voice compression channels. These support the common IP audio codecs G711, G723 and G729a.

For the B5800 Branch Gateway control unit, channels can be added using VCM base cards, BRI combination cards, and ATM combination cards. See System components on page 20 for more information about these cards.

The voice compression channels are used as follows:

Call type	Voice compression channel usage
IP device to non-IP device	These calls require a voice compression channel for the duration of the call. If no channel is available, busy indication is returned to the caller.
IP device to IP device	Call progress tones (for example dial tone, secondary dial tone, etc) do not require voice compression channels with the following exceptions: • Short code confirmation, ARS camp on and account code entry tones require a voice compression channel. • Devices using G723 require a voice compression channel for all tones except call waiting. When a call is connected: • If the IP devices use the same audio codec no voice compression channel is used. • If the devices use differing audio codecs, a voice compression channel is required for each.
Non-IP device to non-IP device	No voice compression channels are required.
Music on Hold	This is provided from the B5800 Branch Gateway TDM bus and therefore requires a voice compression channel when played to an IP device.
Conference resources and IP devices	Conferencing resources are managed by the conference chip which is on the B5800 Branch Gateway TDM bus. Therefore, a voice compression channel is required for each IP device involved in a conference. This includes services that use conference resources such as call listen, intrusion, call recording and silent monitoring.
Page calls to IP dDevice	B5800 Branch Gateway only uses G729a for page calls, therefore only requiring one channel but also only supporting pages to G729a capable devices.
Voicemail services and IP devices	Calls to the B5800 Branch Gateway voicemail servers are treated as data calls from the TDM bus. Therefore calls from an IP device to voicemail require a voice compression channel.
T38 fax calls	In order to use T38 fax connection, B5800 Branch Gateway performs fax tone detection if the analog extension connected to the fax machine is set as “Standard telephone.” If the fax machine does not include an attached handset that is used to make/receive voice calls, then the Equipment Classification of an analog extension connected to the fax machine can be set to **Fax Machine**, which will result in T38 fax connection without fax tone detection and respective signaling renegotiation. Additionally, a new short code feature, Dial Fax, is available.

Measuring channel usage

The IP Office System Status Application can be used to display voice compression channel usage. Within the **Resources** section it displays the number of channels in use. It also displays how often there have been insufficient channels available and the last time such an event occurred.

For the VCM cards, the level of channel usage is also indicated by the LEDs (1 to 8) on the front of the VCM card.

Emergency and power failure ports

B5800 Branch Gateway systems can provide 2 types of analog extension power failure ports as described in the following table.

Type	Description	Provided By:
Switching power failure ports	During normal B5800 Branch Gateway operation these ports can be used for normal analog phone connection. During power failure the port is directly connected to an analog trunk port.	• **Analog phone 8 card** When an analog phone 8 base card is fitted with an analog trunk daughter card, during power failure extension port 8 is connected to analog trunk port 12. • **ATM combination card** On this card, during power failure, extension port 8 is connected to analog trunk port 12.
Emergency only power failure ports	During normal B5800 Branch Gateway operation these ports cannot be used. During power failure the port is directly connected to an analog trunk port.	• **Analog trunk daughter card** Regardless of the card hosting it, during power failure pins 4 and 5 of port 12 are connected to pins 7 and 8.

In all cases these only work with loop-start analog trunks. Any phones connected to these ports should be clearly labeled as power fail extensions in accordance with the appropriate national and local regulatory requirements.

Environmental requirements

The planned location must meet the following requirements. If being installed into a rack system, these are requirements for within the rack:

- Temperature: 0°C to 40°C / 32°F to 104°F.
- Humidity: 10% to 95% non-condensing.
- Check there are no flammable materials in the area.
- Check there is no possibility of flooding.
- Check that no other machinery or equipment needs to be moved first.
- Check that it is not an excessively dusty atmosphere.
- Check that the area is unlikely to suffer rapid changes in temperature and humidity.
- Check for the proximity of strong magnetic fields, sources of radio frequency and other electrical interference.
- Check there are no corrosive chemicals or gasses.
- Check there is no excessive vibration or potential of excessive vibration, especially of any mounting surface.
- Check that where telephones are installed in another building, that the appropriate protectors and protective grounds are fitted (see Out of Building Telephone Installation on page 72).
- Check there is suitable lighting for installation, system programming and future maintenance.
- Check that there is sufficient working space for installation and future maintenance.
- Ensure that likely activities near the system will not cause any problems, e.g. access to and maintenance of any other equipment in the area.
- Where ventilation holes are present on any of the B5800 Branch Gateway units, those holes should not be covered or blocked.
- The surface must be flat horizontal for free-standing or rack mounted installations.

Wall mounting: In additional to the requirements above, the following are applicable to control units that are mounted on the wall.

- Units must only be mounted onto permanent wall surfaces.
- The surface must be vertical and flat.
- Orientation of the unit must be as shown in the section on IP500 Wall Mounting on page 65.
- The appropriate Avaya wall mounting kits must be used.

Note:

See Important safety instructions when using your telephone equipment on page 263 for basic safety precautions to follow when using your telephone equipment.

Space requirements

The B5800 Branch Gateway control unit and external expansion modules are designed to be installed either in a free-standing stack or into a 19-inch rack system. Rack installation requires a rack mounting kit for each control unit and expansion module. See Rack mounting on page 67 for more information. If there are no external expansion modules used in the installation, the control unit can be wall mounted using a wall mounting kit. See Wall mounting on page 65 for more information.

- **Cable clearance**

  Clearance must be provided at the front and rear of all modules for cable access. Allow a minimum clearance of 90mm (3.5 inches).

- **Additional clearance**

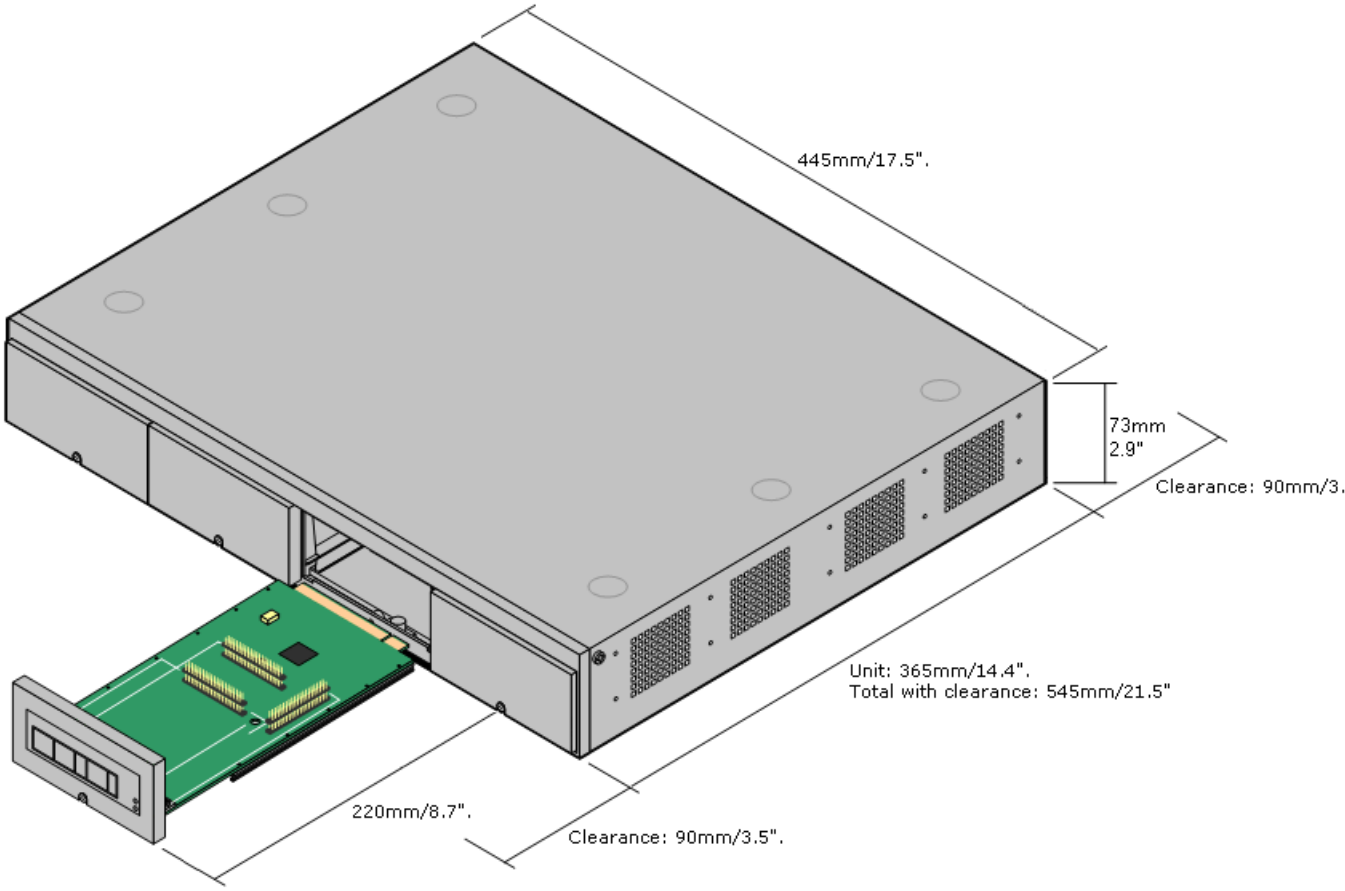
  Care should be taken to ensure that the positioning of the modules does not interrupt air flow and other environmental requirements. The control unit has ventilation slots at the side that must not be blocked. See Environmental requirements on page 47 and Rack space requirements on page 50 for more information.

- **Cable access**

  Power cords must not be attached to the building surface or run through walls, ceilings, floors and similar openings. Installation measures must be taken to prevent physical damage to the power supply cord, including proper routing of the power supply cord and provision of a socket outlet near the fixed equipment or positioning of the equipment near a socket outlet.

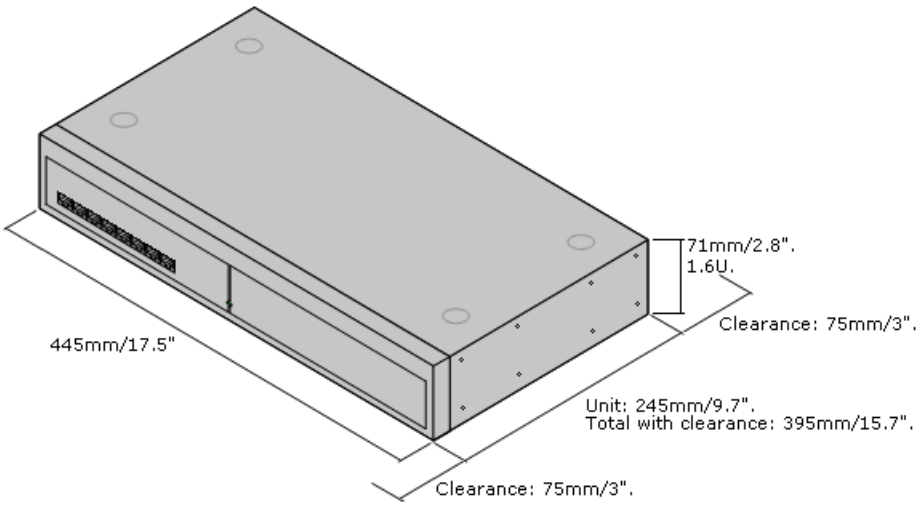
Control unit

When wall mounted, a clearance of 500mm is required on all sides. The ventilation slots on the rear and sides should not be covered or blocked.



External expansion modules

The dimensions below are applicable to all external expansion modules.



Wall mounting space requirements

The control unit can be wall mounted if not using any external expansion modules. A wall mounting kit is required in addition to 4.5mm fixings suitable for the wall type. A clearance of 500mm around the control unit is required. See Wall mounting on page 65 for more information.

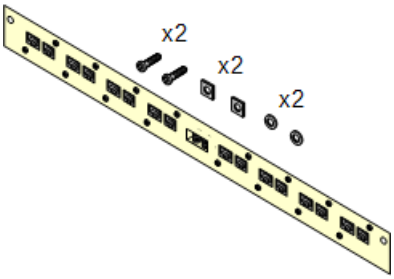
Rack space requirements

The B5800 Branch Gateway control unit and external expansion modules can be rack mounted into standard 19-inch rack systems. Each unit requires a 2U slot space within the rack. Rack mounting requires a rack mounting kit for each control unit and external expansion module. See Rack mounting on page 67 for more information about the rack mounting kit.

Where B5800 Branch Gateway systems are being rack mounted, the effect of conditions within the rack cabinet must be considered. For example the rack temperature may be above the room temperature and airflow within the rack will be restricted. The environmental requirements for the individual control unit and expansion modules are still applicable inside the rack cabinet.

Barrier box rack mounting kit

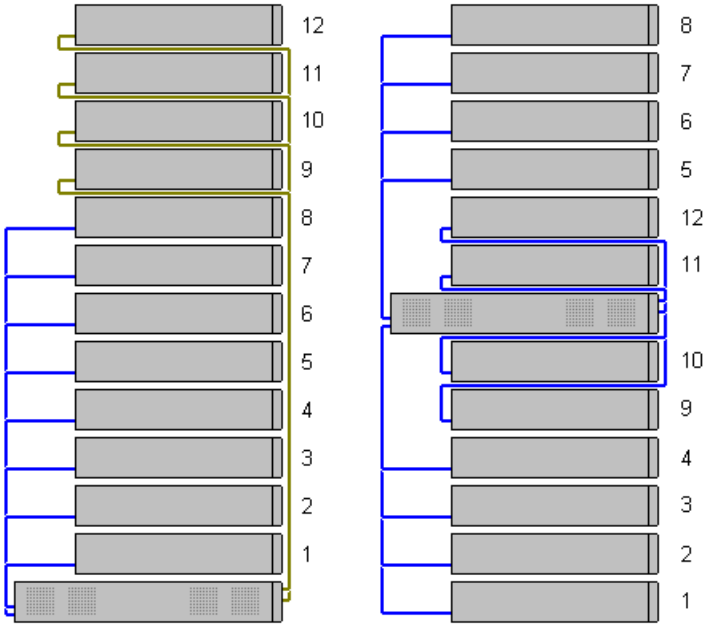
The barrier box rack mounting kit must be used for out-of-building analog phone extensions. This bracket allows up to 8 barrier boxes to be rack mounted and simplifies the number of connections to the protective ground point in the rack. This kit must be used when more than 3 barrier boxes are in use and supports a maximum of 16 barrier boxes for a single external expansion module.



Rack module positioning

The integral expansion ports on a control unit are located on the rear of the unit. An additional 4 expansion ports can be added to the front of the control unit by installing a 4-port expansion card.

- Each external expansion module is supplied with a blue 1 meter (3'3") expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on a 4-port expansion card, a yellow 2-meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. Four yellow cables are supplied with the 4-port expansion card.



Chapter 4: Hardware and software installation

This chapter addresses new installations. If you are upgrading a B5800 Branch Gateway system, see Upgrading an R6.1 system to R6.2 on page 89 or Upgrading an R6.2 system with an R6.2 service pack on page 97.

All hardware components should be turned off while they are installed and connected. Once the installation is complete, the system is turned on. The control unit will then upgrade all of the connected components, including phones, to the appropriate level of firmware. In addition, when the system is turned on, it should not be connected to the customer's data network. This ensures that the control unit will default to known default IP address settings (unless you have pre-loaded the System SD card with a configuration file with different settings).

B5800 Branch Gateway R6.2 provides the B5800 Branch Gateway Initial Installation utility. This utility provides a default configuration and security settings that minimize initial installation activities and maximize security. The system must be configured with the default settings before the system can be administered by Avaya Aura® System Manager. This utility is used for new installations and after an R6.1 to R6.2 upgrade to enable System Manager administration of the B5800 Branch Gateway. For more information, see Using the Initial Installation Utility on page 121.

Installation checklist

Use this checklist to monitor your progress as you install a B5800 Branch Gateway system.

#	Description	Section	✔
1	Review the prerequisites.	See Prerequisites on page 35.	
2	Review the Installation requirements.	See Installation requirements on page 41.	
3	Review the required tools and equipment.	See Tools and equipment required on page 54.	
4	Unpack the equipment.	See Unpacking equipment on page 55.	
5	If you want to pre-configure the system, there are several tasks you can perform to configure the	See SD card preparation on page 56.	

#	Description	Section	✔
	SD card before it is installed in the control unit.		
6	Prepare the base and trunk cards and install them in the control unit.	See Base and trunk card installation on page 59.	
7	Do one of the following: • Install the control unit on the wall. • Install the control unit in a rack.	See one of the following: • Wall mounting on page 65. • Rack mounting on page 67.	
8	Connect the external expansion modules.	See External expansion modules on page 69.	
9	Connect the control unit and external expansion modules to a functional ground.	See Grounding on page 71.	
10	Install the B5800 Branch Gateway administration applications on the installer PC.	See Installing the administration applications on page 79.	
11	Connect the PC to the control unit.	See Installer PC connection on page 79.	
12	Apply power to the system.	See Applying power to the system on page 81.	
13	Use the initial installation utility to configure a default configuration and security settings.	See Using the Initial Installation Utility on page 121.	
15	Connect the control unit to the network.	See Connecting the control unit to the network on page 86.	
18	Connect the phones.	See Connecting phones on page 87.	

Tools and equipment required

Following is a general summary of the tools required. Additional tools and equipment are required for wall and/or rack mounting and to fashion ground cable connections suitable to local requirements.

- **Tools required**
  - 5mm Flat-blade screwdriver
  - Crosshead screwdriver

- Anti-static wrist strap and ground point
- RJ45-RJ45 ethernet LAN cable
- M4 cross-head screwdriver
- Tools suitable for crimping a cable spade
- If wall mounting, drills and tools for wall mounting fixtures

• **Additional parts required**

In addition to orderable system equipment, the following items are required.

- 14AWG solid copper wire for ground connection of control units and expansion modules
- Cable sleeve matching local regulator requirements for ground wires. Typically green for a functional ground and green/yellow for a protective ground.
- If wall mounting, additional 4.5mm diameter fixtures and fittings suitable for the wall type
- Cable ties and labels for tidying and identifying cables

• **PC requirements**

- Windows PC with the administration software installed. See PC requirements on page 78.
- SD card reader

Unpacking equipment

About this task

Use the following procedure when unpacking any equipment supplied by Avaya or an Avaya reseller or distributor. Have the equipment order checklist available as you unpack the equipment to ensure you have all parts and equipment ordered.

Procedure

1. **Check for package damage**

   Before unpacking any equipment, check for any signs of damage that may have occurred during transit. If any damage exists bring it to the attention of the carrier.

2. **Check the correct parts have been delivered**

   Check all cartons against the packing slip and ensure that you have the correct items. Report any errors or omissions to the equipment supplier.

3. **Retain all packaging and documentation**

   While unpacking the equipment, retain all the packaging material. Fault returns are accepted only if repackaged in the original packaging. If performing a staged

installation, the original packaging will also assist when repacking equipment to be moved to the final install site.

4. **Ensure that anti-static protection measures areobserved**

   Ensure that anti-static protection measures are observed at all times when handling equipment with exposed electrical circuit boards.

5. **Check all parts**

   Visually inspect each item and check that all the necessary documentation and accessory items have been included. Report any errors or omissions to the dealer who supplied the equipment.

6. **Check all documentation**

   Ensure that you read and retain any documentation included with the equipment.

SD card preparation

B5800 Branch Gateway control units are supplied with no installed firmware or configuration. When first powered up, the control unit loads and installs the necessary firmware from the B5800 Branch Gateway System SD card that has been installed in the control unit. A default configuration is then created that matches the cards installed in the control unit and external expansion modules attached.

You can perform the following tasks prior to installing the B5800 Branch Gateway System SD card in order to pre-configure the system.

- See Upgrade the Card Firmware on page 56
- See Creating a configuration file on page 57.
- See Adding a configuration file on page 58.
- See Adding music-on-hold files on page 58.
- See Add a 9600 Screen Saver Image File on page 59.

For more information about SD cards, see SD Card Management on page 241.

Upgrading the card firmware

About this task

This process creates the folder structure on the SD card and copies the firmware files from those installed with Manager onto the SD card. This includes the binary files for the B5800 Branch Gateway system and any external expansion modules and phones. It also includes the prompt files for embedded voicemail operation.

This process can be used to upgrade an existing SD card to match the file set installed with Manager. The card installed in the System SD slot must be an Avaya SD Feature Key card. The card must be correctly formatted.

If the card contains any dynamic system files, for example SMDR records, they are temporarily backed up by Manager and then restored after the card is recreated.

Procedure

1. Insert the SD card into a card reader on the Manager PC.

   Note:

   Do not remove the SD card. Removing the SD card will interrupt the upgrade.
2. Using Manager, select **File** > **Advanced** > **Recreate IP Office SD Card**.
3. Select **Avaya Branch Gateway**.
4. Browse to the card location and click **OK**.
   Manager starts creating folders on the SD card and copying the required files into those folders. This process takes approximately 15 minutes. Do not remove the SD card until Manager shows a message that the recreation has finished.

Creating a configuration file

About this task

Manager can be used to create a new configuration file without connecting to a B5800 Branch Gateway system. This allows the creation of a configuration prior to installing the system. The configuration file can be loaded on the System SD card before the card is installed. The configuration file specifies the system's location, trunk cards, control unit, and expansion modules.

- The configuration created must match the physical equipment in the B5800 Branch Gateway system for which the configuration will be loaded. If they do not match, the system may reset and experience other problems.
- The configuration creation tool includes all control units, external expansion modules and trunk cards supported by B5800 Branch Gateway. It is your responsibility to confirm the B5800 Branch Gateway equipment that is supported in your location.

Procedure

1. Start Manager with no configuration loaded into Manager.
2. Click on **Create an Offline Configuration** in the simplified view.
3. Select the type of configuration that you want to create.
4. When completed, click **OK**.
   Manager will create and load the configuration.

5. Edit the configuration to match the customer requirements.
   This can include importing information from prepared CSV files.

   Note:

   For information about CSV files, see the Help available in the Manager application. From Manager, select **Help > Contents**. In the Manager Help window, in the left navigation pane, expand **IP Office Configuration Mode** and then expand **Editing Configuration Settings**. Then click **Importing and Exporting Settings**.

6. When completed, select **File** > **Save Configuration As**.

Adding a configuration file

About this task

Use this procedure to add a configuration file on the System SD card. That configuration file will then be used when the B5800 Branch Gateway system is started.

Procedure

1. Create an offline configuration that matches the customer requirements and the equipment that will be installed in the B5800 Branch Gateway system. See Creating a configuration file on page 57.
2. Rename the configuration file **config.cfg**.
3. Using a card reader, copy the file into the **/system/primary** folder on the System SD memory card.

Adding music-on-hold files

About this task

By default B5800 Branch Gateway uses internal music-on-hold by uploading a music file. You can load a file onto the System SD card prior to installing it in the control unit

The file must be of the following format and must be called **holdmusic.wav**.

Property	Value
File Type	WAV
Bit Rate	128kbps
Audio sample size	16 bit

Property	Value
Channels	1 (mono)
Audio Sample Rate	8 kHz
Audio Format	PCM
Length	Up to 90 seconds.

Procedure

1. Rename the music file **holdmusic.wav**.
2. Using a card reader, copy the file into the **/system/primary** folder on the System SD memory card.
3. If the B5800 Branch Gateway system is configured for additional music-on-hold files (up to 3 additional files), copy those files to the same location.

   The name of the additional files must match those specified in the B5800 Branch Gateway system configuration.

9600 series phones screen saver file

When idle, 9600 Series phones can timeout and display a screen saver image. A file, **96xxiposs.jpg**, is present on the cards by default.

You can replace this file with your own branded file. The file should be smaller than the screen size on 9600 Series phones in order for the image to move around the screen.

Base and trunk card installation

The base cards and trunk daughter cards should be fitted before power is applied to the control unit. Ensure that cards are inserted in the order that matches the planned or pre-built configuration. In general, the following applies to card installation:

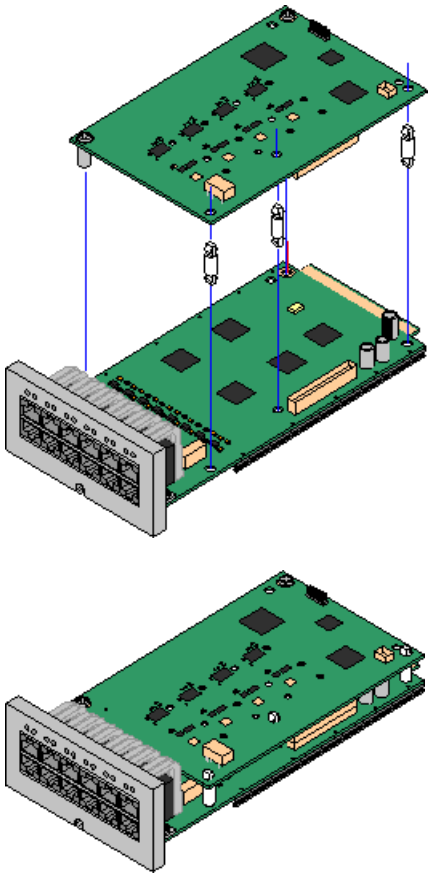
- Cards can be fitted in any order into any available slots. The only exception is the 4-port expansion card which can only be installed in right-hand slot 4.
- It is recommended that cards are fitted from left to right.
- There are restrictions to the number of supported cards of some types. When a limit is exceed, the right-most card of that type will not function.
- Ensure that you use the labels supplied to identify the card fitted into the control unit.

⚠ Warning:

- Correct anti-static protection steps should be taken before handling circuit boards.
- Cards must never be added or removed from the control unit while it has power connected.

Trunk daughter card preparation

Trunk daughter cards can be fitted to any base card except the legacy card carrier. For combination cards, the trunk daughter card is pre-installed and cannot be changed.



⚠ Warning:

Correct anti-static protection steps should be taken while handling circuit boards.

Parts and equipment required

- Base card (except the legacy card carrier)
- Trunk daughter card
- 3 stand-off pillars (these are supplied with the trunk daughter card)

Tools required

- 5mm Flat-blade screwdriver
- Anti-static wrist strap and ground point

Installing a trunk daughter card

Procedure

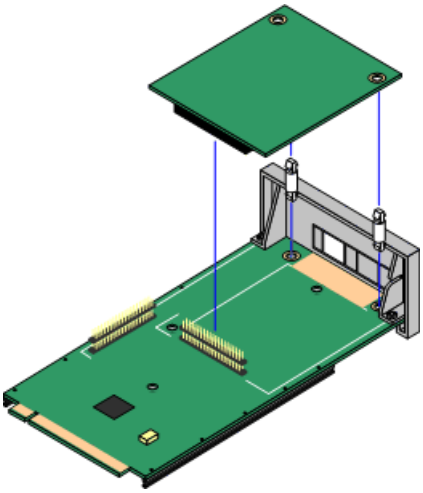
1. Check that correct cards have been supplied.
2. Ensure that you are wearing an anti-static wrist strap connected to a suitable ground point.
3. On the base card, identify the position of the 3 holes for the plastic pillars for the trunk daughter card.

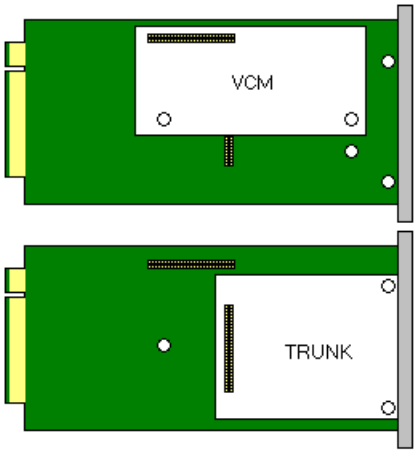
   These are along the same edge as the card connector.
4. Fit the stand-off pillars to the base card.
5. If there is a clip-on metal shield over the connector block on the base card, remove it.
6. Using minimal force and checking that the pins are correctly located, push the trunk card onto its connector block and the stand-off pillars.
7. Check that the card connector has snapped into position.
8. Using the washers and screws provided, secure the metal stand-off pillars to the base card.
9. From the set of labels that are supplied with the trunk daughter card, fit the appropriate label to the front of the base card.

Legacy carrier card preparation

A legacy carrier card can be used to fit VCM cards into the B5800 Branch Gateway control unit. Up to 2 legacy carrier cards can be inserted. The following trunk and VCM cards are supported. Cards not listed are not supported.

• PRI T1 • Dual PRI T1 • PRI 30 E1 (1.4) • Dual PRI E1	• PRI 30 E1R2 RJ45 • Dual PRI E1R2 RJ45 • BRI-8 (UNI) • ANLG 4 UNI (US only)	• VCM 4 • VCM 8 • VCM 16 • VCM 24 • VCM 30





⚠ Warning:

Correct anti-static protection steps should be taken while handling circuit boards.

Parts and equipment required

- Legacy carrier card
- VCM card
- 2 plastic stand-off pillars per card
- Trunk cards are supplied with a replacement blanking plate which is not required.

Tools required

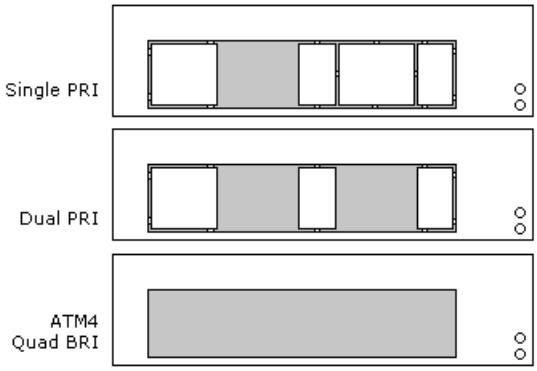
- 5mm Flat-blade screwdriver
- Anti-static wrist strap and ground point

Installing a legacy carrier card

Procedure

1. Check that correct cards have been supplied.
2. Ensure that you are wearing an anti-static wrist strap connected to a suitable ground point.
3. On the carrier card identify the position of the jumper block and stand-off pillar holes for the IP400 card.

   The peg holes are labeled as VCM or TRUNK.
4. If fitting an IP400 trunk card, identify which of the plastic snap-off panels on the front of the carrier card need to be removed to allow the trunk cable connections.



5. Carefully remove those panels.
6. Fit the stand-off pillars to the legacy carrier card.
7. Using minimal force and checking that the pins are correctly located, push the IP400 card onto its jumper and the stand-off pillars.

Base card insertion

Having prepared each base card by adding the trunk daughter cards or legacy carrier cards, the base card can be inserted into the control unit.

⚠ Warning:

- Correct anti-static protection steps should be taken before handling circuit boards.
- Cards must never be added or removed from the control unit while it has power connected.

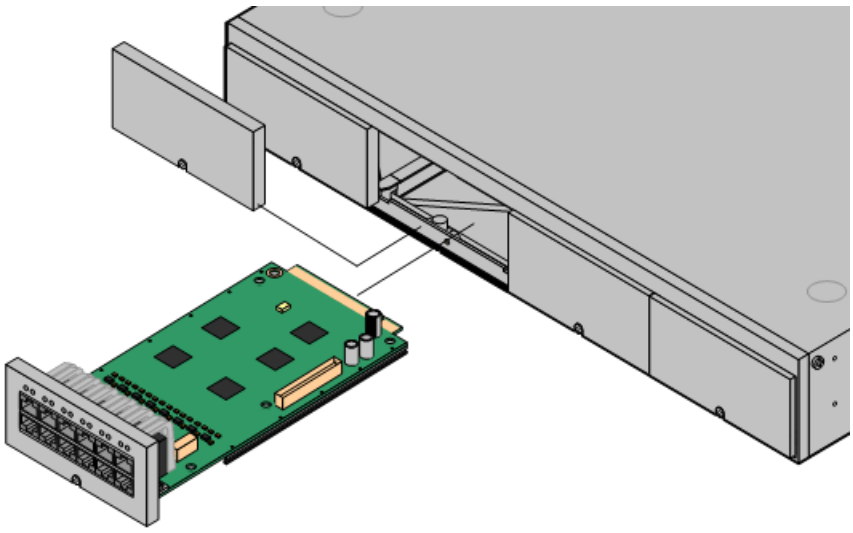
- **Tools required**
  - 5mm Flat-blade screwdriver
  - Anti-static wrist strap and ground point

Installing a base card

Procedure

1. Check that there is no power to the control unit.
2. Using a flat-bladed screwdriver, remove the cover from the slot on the front of the control unit that will be used for each card being installed.

   This cover is no longer required but should be retained until installation has been completed.



3. Allowing the card to rest against the bottom of the slot, begin sliding it into the control unit.
4. When half inserted, check that the card rails have engaged with the slot edges by trying to gently rotate it. If the card rotates, remove it and begin inserting it again.

   The card should slide in freely until almost fully inserted.

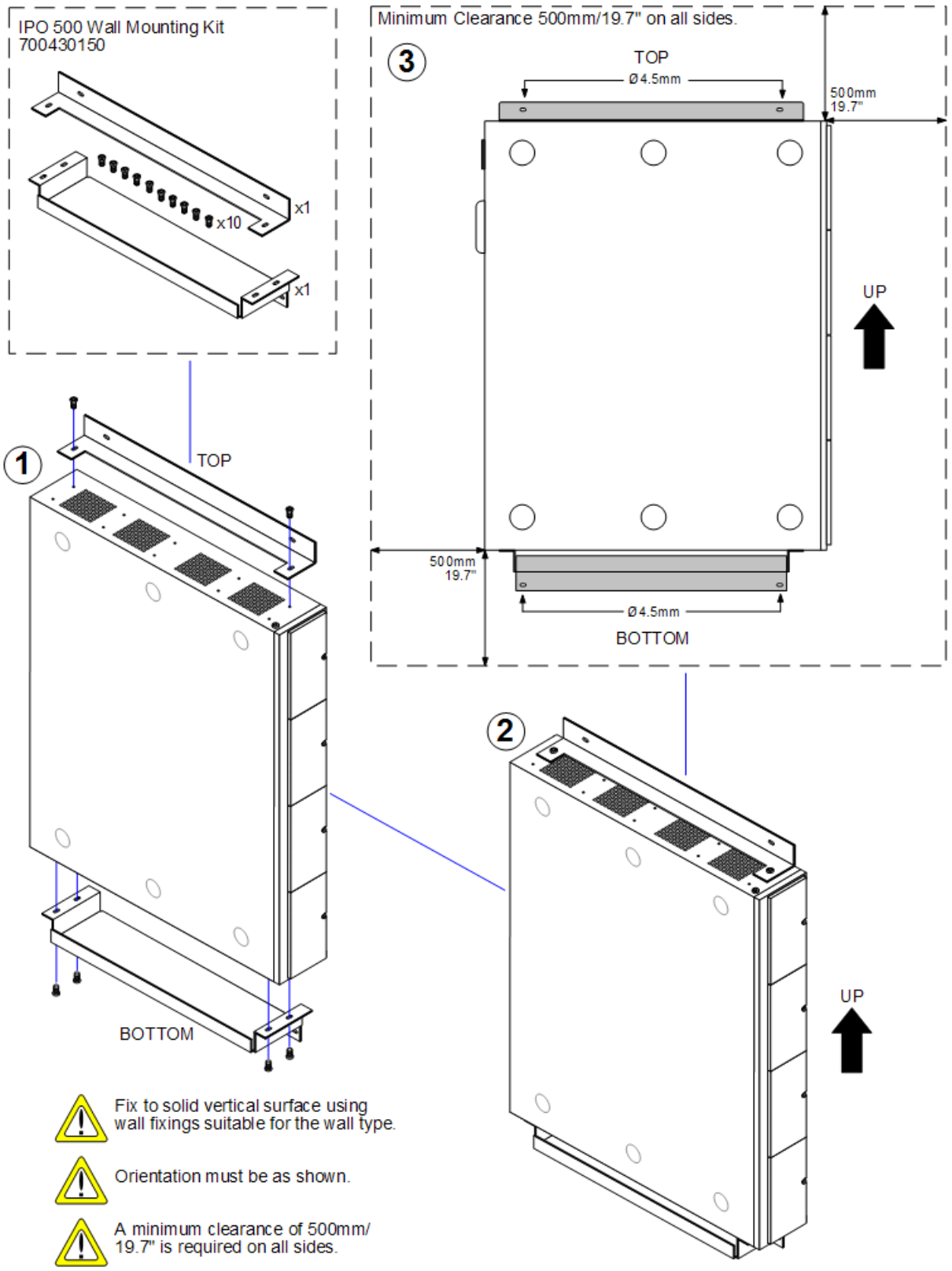
5. At this point apply pressure at the base of the front of the card to complete insertion.
6. Using a flat-bladed screwdriver secure the card.

Wall mounting

B5800 Branch Gateway control units can be wall mounted. This requires a wall mounting kit plus additional 4.5mm fixtures and fittings suitable for the wall type. The wall mounting kit includes two brackets, one top and one bottom.

In addition to the existing environmental requirements on page 47, the following requirements apply when wall mounting a unit:

- The wall surface must be vertical, flat and vibration free.
- The brackets must be used as shown, with the deeper tray-like bracket used at the bottom of the wall mounted control unit.
- Only the screws (M3 x 6mm) provided with the mounting kit should be used to attach the brackets to the control unit.


IPO 500 Wall Mounting Kit
700430150
x1
x10
x1
Minimum Clearance 500mm/19.7" on all sides.
3
TOP
Ø4.5mm
500mm
19.7"
UP
500mm
19.7"
Ø4.5mm
BOTTOM
1
TOP
BOTTOM
2
UP
Fix to solid vertical surface using wall fixings suitable for the wall type.
Orientation must be as shown.
A minimum clearance of 500mm/ 19.7" is required on all sides.

Rack mounting

The B5800 Branch Gateway control unit and external expansion units can be rack mounted into 19-inch rack systems. This requires a rack mounting kit for each unit.

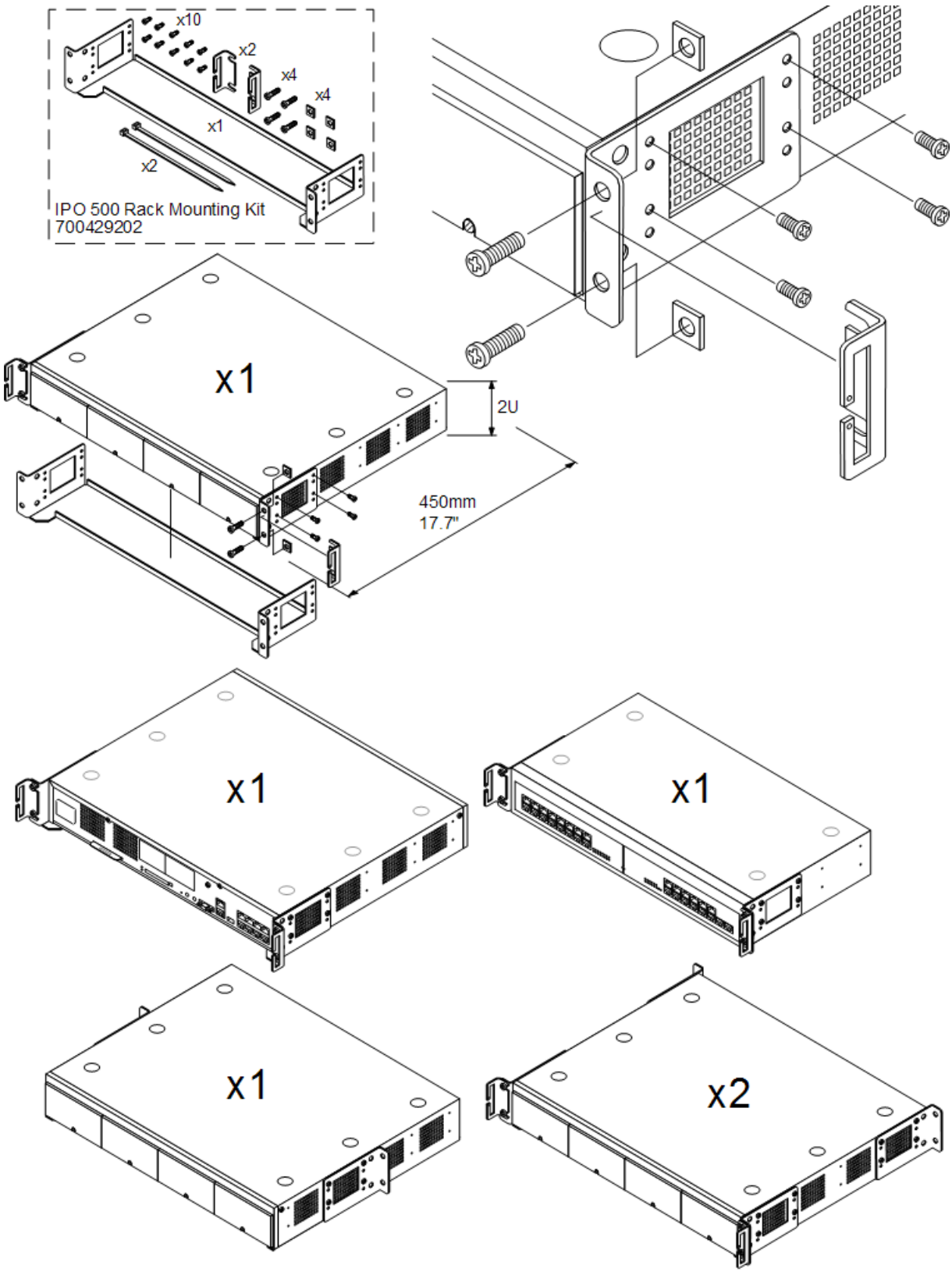
The rack mounting kit includes:

- A rack mounting bracket and screws for attachment of the bracket to the unit
- Nuts and bolts for rack attachment
- Brackets and cable ties for cable tidying

Environmental requirements

In addition to the environmental requirements on page 47, the following factors must be considered when rack mounting a unit:

- Rack positioning — Ensure compliance with the rack manufacturers safety instructions. For example check that the rack legs have been lowered and fixing brackets have been used to stop toppling.
- Elevated operating ambient — If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
    - Operating temperature: 0°C (32°F) to 40°C (104°F).
    - Operating humidity: 10% to 95% non-condensing.
- Reduced air flow — Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised. Proper ventilation must be maintained. The side ventilation slots on the control unit should not be covered or blocked.
- Mechanical loading — Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit overloading — Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable earthing — Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).



- **Important:**

  Only the screws (M3 x 6mm) provided with the mounting kit should used to attach the

brackets to the control unit. As indicated in the diagram, the rack mounting bracket can be used in several positions on the unit.

External expansion modules

External expansion modules should be connected to the control unit before power is applied to the control unit. Ensure that modules are attached in the order that matches the planned or pre-built configuration.

External expansion modules connect to the control unit using an expansion interconnect cable. Each module is supplied with an expansion interconnect cable and a power supply unit. An appropriate local specific power cord for the power supply unit must be ordered separately.

- Each external expansion module is supplied with a blue 1 meter (3'3") expansion interconnect cable. This cable must be used when connecting to expansion ports on the rear of a control unit.
- When connecting to expansion ports on a 4-port expansion card, a yellow 2-meter (6'6") expansion interconnect cable can be used in place of the standard blue cable. Four yellow cables are supplied with the 4-port expansion card.

Installation requirements

- Installation space either on or under the control unit
- Switched power outlet socket
- Available EXPANSION port on the control unit
- Functional grounding requirements — connection of a functional ground is:
  - recommend for all modules
  - mandatory for analog trunk modules
- Protective grounding requirements — connection of a protective ground via surge protection equipment is:
  - mandatory for analog trunk modules in the Republic of South Africa
  - mandatory for digital station and phone modules connected to out-of-building extensions
  - mandatory for digital station V2 and phone V2 modules

Tools required

- Manager PC
- Tools for rack mounting (optional)

Parts and equipment required

- External expansion module — each module is supplied with a suitable external power supply unit and a 1m blue interconnect cable. 2m yellow interconnect cables are supplied with the 4-Port expansion card and should only be used with that card.
- Power cord for the power supply unit
- Rack mounting kit (optional)
- Cable labeling tags

Connecting external expansion modules

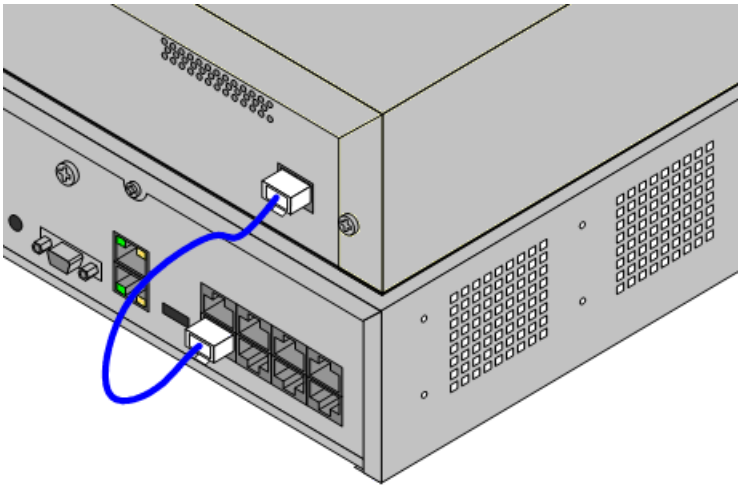
About this task

Note:

External expansion modules should not be attached to a control unit that has power.

Procedure

1. If the system is being installed in a rack, attach the rack mounting kit to the expansion module. See Rack mounting on page 67.
2. Attach the external expansion module's power supply but do not switch power on.
3. Connect the expansion interconnect cable from the module's EXPANSION port to the EXPANSION port on the control unit. Make careful note of the port used and include this detail on the cable label and any other system records.



Grounding

Use of ground connections reduces the likelihood of problems in most telephony and data systems. This is especially important in buildings where multiple items of equipment are interconnected using long cable runs, for example phone and data networks.

All control units and external expansion modules must be connected to a functional ground. Where the unit is connected to a power outlet using a power cord with an earth lead, the power outlet must be connected to a protective earth.

In some cases, such as ground start trunks, in addition to being a protective measure this is a functional requirement for the equipment to operate. In other cases it may be a locale regulatory requirement and or a necessary protective step, for example areas of high lightning risk.

⚠ Warning:

During installation do not assume that ground points are correctly connected to ground. Test ground points before relying on them to ground connected equipment.

Additional protective equipment

In addition to grounding, additional protective equipment is required in the following situations.

- On any digital station or phones external expansion module connected to an extension located in another building. See Out of Building Telephone Installations on page 72.
- In the Republic of South Africa, on all analog trunk external expansion modules (ATM16) and on any control units containing an analog trunk cards (ATM4/ATM4U).

Tools required

- M4 cross-head screwdriver
- Tools suitable for crimping a cable spade

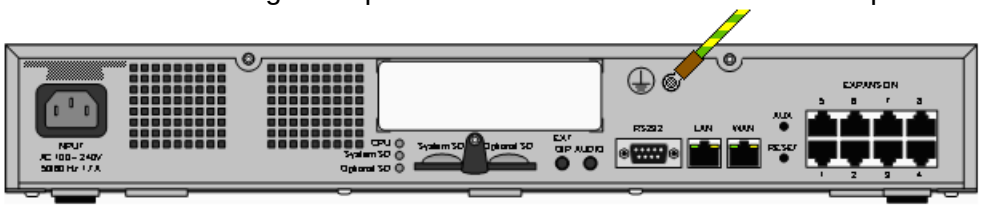
Parts and equipment required

- 14AWG solid copper wire for ground connection
- Cable sleeve matching local regulator requirements. Typically green for a functional ground and green/yellow for a protective ground.

The ground point on control units and expansion modules are marked with a ⏚ or ⏚ symbol. Ground connections to these points should use a 14 AWG solid wire with either a green sleeve for a functional ground or green and yellow sleeve for a protective ground.

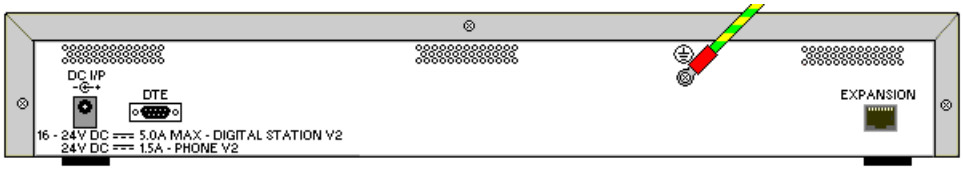
B5800 Branch Gateway control unit

On control units the ground point is located above the RS232 DTE port.



External expansion modules

On expansion modules, the ground point is a 4mm screw located towards the right on the rear of the module.



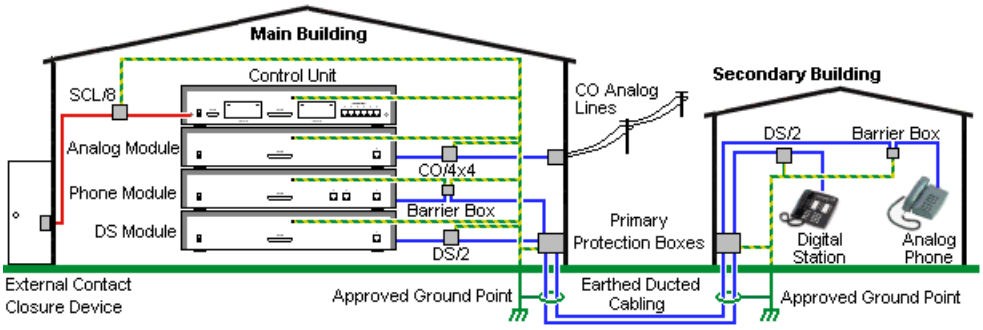
On some older modules, the dedicated ground point screw is not present. In those cases, the top-center cover fixing screw (3mm) can be used as an alternative ground connection point. A toothed washer should be added to ensure good contact.

Out-of-building connections/lightning protection

The following are the only supported scenarios in which wired extensions and devices outside the main building can be connected to the B5800 Branch Gateway system. In these scenarios, additional protection in the form of protective grounding and surge protectors must be fitted.

⚠ Warning:

The fitting of additional protection does not remove the risk of damage. It merely reduces the chances of damage.



- Cables of different types, for example trunk lines, phone extensions, ground and power connections, should be kept separate.
- All cabling between buildings should be enclosed in grounded ducting. Ideally this ducting should be buried.
- A Primary Protection Box must be provided at the point where the cables enter the building. This should be three point protection (tip, ring and ground). Typically this would be gas tube protection provided by the local telephone company. The ground wire must be thick enough to handle all the lines being affected by indirect strike at the same time.

Connection type	Protection device type	Requirement
DS phone extensions External expansion module DS ports only.	**ITWLinx towerMAX DS/2** Supports up to 4 connections. (This device was previously referred to as the Avaya 146E.)	• Connection from the expansion module to the phone must be via a surge protector at each end and via the primary protection point in each building. • The expansion module, control unit, and IROB devices must be connected to the protective ground point in their building. • The between building connection must be via earthed ducting, preferable underground. The cable must not be exposed externally at any point.
Analog phone extensions Phones external expansion module (POT or Phone) ports only.	**Barrier box** Supports a single connection. Maximum of 16 on any expansion module.	
Analog trunks	**ITWLinx towerMAX CO/4x4** Supports up to 4 two-wire lines. (This device was previously referred to as the Avaya 146C.)	For installations in the Republic of South Africa, the fitting of surge protection on analog trunks is a requirement. For other locations where the risk of lightning strikes is felt to be high, additional protection of incoming analog trunks is recommended.

Connection type	Protection device type	Requirement
External output switch	**ITWLinx towerMAX SCL/8** (This device was previously referred to as the Avaya 146G.)	Connections from an Ext O/P port to an external relay device must be via a surge protector.

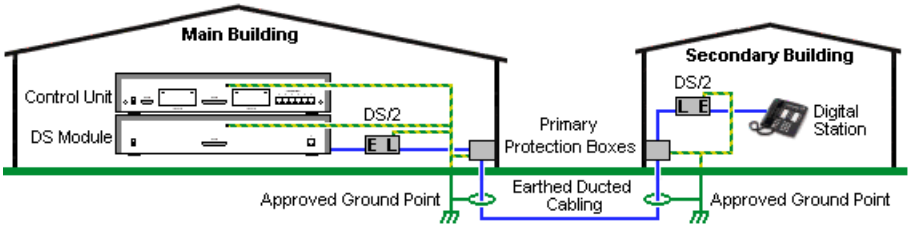
The towerMAX range of devices are supplied by ITWLinx (http://www.itwlinx.com).

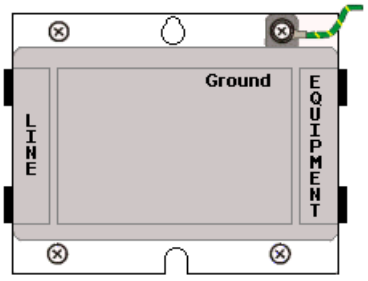
DS phone IROB installation

When digital phone extensions are required in another building, additional In-Range Out-Of-Building (IROB) protective equipment must be used. For phones connected to B5800 Branch Gateway DS ports, the supported device supplied by ITWLinx is a towerMAX DS/2 module. This IROB device was previously referred to by Avaya as the 146E IROB.

The protection device should be installed as per the instructions supplied with the device. The ground points on the control unit and the DS modules must be connected to a protective ground using 18AWG wire with a green and yellow sleeve.

Typically the IROBs 2 RJ45 EQUIPMENT ports are straight through connected to the 2 RJ45 LINE ports. This allows existing RJ45 structured cabling, using pins 4 and 5, to be used without rewiring for up to two DS connections. However each of these ports can be used to connect a second extension using pins 3 and 6.



LINE		Signal		EQUIPMENT	
RJ45 8 1	1	Not used		1	RJ45 8 1
	2	Not used		2	
	3	Ring II (Optional)		3	
	4	Ring I		4	
	5	Tip I		5	
	6	Tip II (Optional)		6	
	7	Not used		7	
	8	Not used		8	

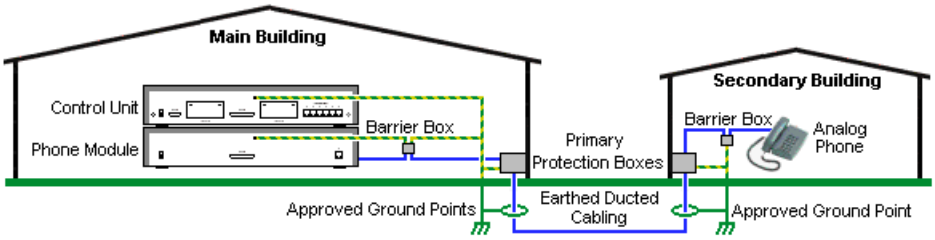
Analog phone barrier boxes

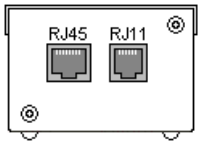
Where analog phone extensions are required in another building, phone barrier boxes and protective earth connections must be used .

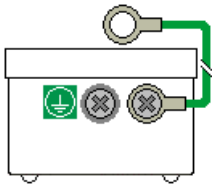
⚠ Warning:

PHONE (POT) ports on the front of control units must not be used for extensions that are external to the main building.

- The correct B5800 Branch Gateway barrier boxes must be used. These modules have been designed specifically for the signalling voltages used by the B5800 Branch Gateway system:
  - Only the B5800 Branch Gateway phone barrier box should be used with phone V1 modules.
  - Only the B5800 Branch Gateway phone barrier box V2 should be used with phone V2 modules.
  - No other type of analog phone barrier box should be used.
  - Where more than 3 barrier boxes are required in a building, they must be rack mounted using a barrier box rack mounting kit. See Rack mounting barrier boxes on page 76.
  - A maximum of 16 barrier boxes can be used with any phone module.
  - The phone barrier box does not connect the ringing capacitor in phone V1 modules.



Main Building	Barrier Box	Secondary Building
• **RJ11** — Connect to PHONE (POT) port on the Phone module using cable supplied with the barrier box. • **RJ45** — Connect to the secondary building barrier box via primary protection in both buildings.		• **RJ11** — Connect to analog phone. Cable not supplied. • **RJ45** — From main building via primary protection in both buildings.

Main Building	Barrier Box	Secondary Building
• **Center screw** — Connect to main building protective ground (or ground terminal of Barrier Box Rack Mounting Kit). Use 18AWG (minimum) wire with a green and yellow sleeve. • **Right-hand screw** — Connect to ground point on Phone module using ground cable supplied with barrier box.		• **Center screw** — Connect to main building protective ground. Use 18AWG (minimum) wire with a green and yellow sleeve. • **Right-hand screw** — Not used.

The following wires must be kept apart, that is, the wires cannot be routed in the same bundle:

- Earth leads from the barrier box to the phone modules.
- Internal wires, for example extension leads going directly to the phone modules.
- Wires from external telephone going directly to the barrier boxes.

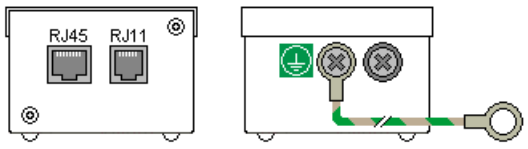
Rack mounting barrier boxes

About this task

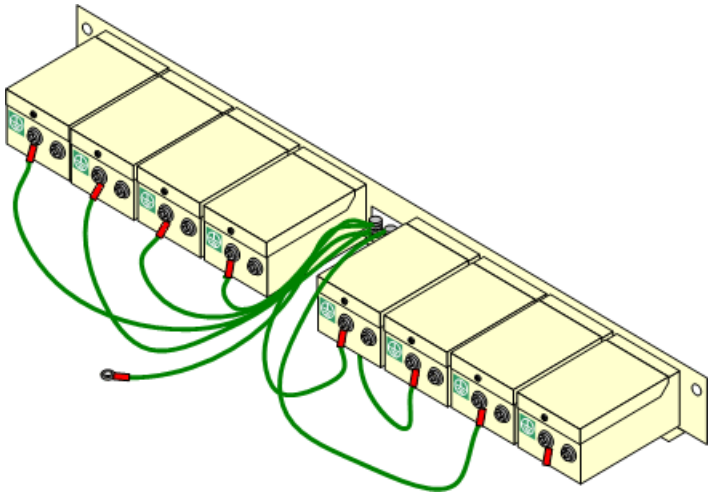
Where more than 3 phone barrier boxes are used they must be rack mounted. The Barrier Box Rack Mounting Kit (SAP Code 700293905) supports up to 8 phone barrier boxes.

Procedure

1. Unscrew the two screws arranged diagonally at the front of each barrier box and use these same screws to reattach the barrier box to the rack mounting strip.
2. Each barrier box is supplied with a solid green ground wire connected to its functional ground screw. Remove and discard this wire.
3. Connect a green/yellow ground wire to the protective earth screw in the center of the point on the back of the barrier box.



4. The rack mounting strip has threaded M4 earthing pillars. Connect the other end of the barrier box ground wire, using M4 washers and nuts, to the earthing pillar on that side of the rack mounting strip.



5. Using 14AWG wire with green and yellow sleeve, connect one of the earthing pillars to the buildings protective earth.
6. Using 14AWG wire with green and yellow sleeve, connect the other earthing pillar to the phone module.
7. Ensure that the following wires are not routed together in the same bundle:
    - Earth lead from the barrier box to the phone module.
    - Internal wires, e.g. wires going directly to the phone module.
    - Wires from external telephone going directly to the barrier boxes.

Administration software suite

The IP Office administration software applications are installed on the installation PC. They are used by installers and maintainers to configure, manage, and monitor the B5800 Branch Gateway system.

The IP Office administration applications are:

- **Manager**

  IP Office Manager is used to access all parts of the B5800 Branch Gateway configuration. Different levels of access can be defined to control which parts of the configuration the Manager user can view and alter. Manager is also used to upgrade the system software files.

- **System Status**

  The IP Office System Status application is a monitoring and reporting tool that provides a wide range of information about the current status of the system. It can report the available resources and components within the system and details of calls in progress.

Details of the number of alarms are recorded and the time and date of the most recent alarms.

- **System Monitor**

  The IP Office System Monitor application is a tool that shows details of all activity on the B5800 Branch Gateway system. Because of the level of detail, interpretation of System Monitor traces requires a high-level of data and telephony protocol knowledge. Installers and maintainers must understand how to run System Monitor when necessary as Avaya may request copies of System Monitor traces to resolve support issues.

PC requirements

The minimum Microsoft® Windows® PC requirements for the B5800 Branch Gateway system tools are provided in the following table. If other applications are to be installed on the PC then those individual requirements should also be met.

Requirement	Minimum	Recommended
Processor	600MHz Pentium or AMD Opteron, AMD Athlon64, AMD Athlon XP.	800MHz Pentium or AMD Opteron, AMD Athlon64, AMD Athlon XP.
RAM	128MB	256MB
HD Space	1GB - 800MB for .NET2, 200MB for Manager.	1.4GB - 800MB for .NET2, 600MB for the full B5800 Branch Gateway Admin suite.
Display	800 x 600 - 256 Colors	1024 x 768 - 16-bit High Color
Operating System	Supported on Windows® XP Pro, Windows® Vista, Windows® 7, Windows® 2003 and Windows® 2008. • 32-bit and 64-bit versions are supported. • Vista support is only on Business, Enterprise and Ultimate versions. • Windows 7 support is only on Professional, Enterprise and Ultimate versions.	

Installing the administration applications

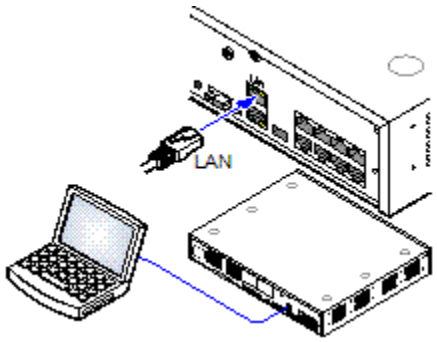
Procedure

1. Using the **Add or Remove Programs** option in the Windows Control Panel, check that the PC does not have an earlier version of the B5800 Branch Gateway Administration Suite installed. If there is, uninstall it.
2. Insert the B5800 Branch Gateway Administrator Applications DVD.
3. Select B5800 Branch Gateway Administration Suite.
4. Double-click on **setup.exe**.
5. Select the language you want to use for the installation process.
   This does not affect the language used by Manager when running.
6. Click **Next**.
7. Select who should be able to run the Administration Suite applications.
8. Click **Next**.
9. If required, select the destination to which the applications should be installed.
   It is recommended that you accept the default destination.
10. Click **Next**.
    The Custom Setup window appears.
11. Select the applications that you want to install. At a minimum select **System Monitor** and **Manager**.
    When you select an application, a description of the application appears. Click on the ▾ next to each application to change the installation selection.
12. Click **Next**.
13. Click **Install**.
    Installation of Windows .Net2 components may be required. If dialogs for this appear, follow the prompts to install .Net.
14. If requested, reboot the PC.

Installer PC connection

During installation it is recommended that the B5800 Branch Gateway control unit be started without it being connected to any network. That ensures that the B5800 Branch Gateway defaults to a known set of IP address settings.

The B5800 Branch Gateway control unit is connected to the PC with a standard RJ45–RJ45 LAN cable.



Connecting the PC directly to the control unit

About this task

The default address for a B5800 Branch Gateway control unit LAN port is 192.168.42.1/255.255.255.0. Use this procedure to change the TCP/IP properties for the LAN port on the PC and directly connect the PC to the control unit.

Procedure

1. Change the TCP/IP properties of the LAN port on the PC to the following:
   - Fixed IP address: 192.168.42.203
   - Subnet mask: 255.255.255.0
   - Default gateway: 192.168.42.1

   Note:

   While setting the PC to be a DHCP client could be used, this is not recommended for performing more advanced functions such as firmware upgrades.
2. Connect the LAN cable from the PC LAN port to the LAN or LAN1 port on the control unit.
3. Check that the orange LED lamp on the control unit LAN port is on.

   The green LED may also be flickering. This indicates traffic across the LAN connection.
4. To test the connection before running Manager or the System Status application, do the following:
   a. Select **Start** > **Run**.
   b. Enter `cmd`.
   c. In the command window that appears, enter `ping 192.168.42.1`.

The results should show a number of ping replies from the B5800 Branch Gateway . This confirms basic communication between the Manager PC and the B5800 Branch Gateway .

d. If there are no ping replies, enter `ipconfig`.

   The results should list the IP address settings of the Manager PC as required above.

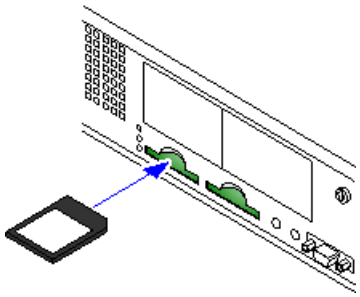
e. If the IP address settings of the Manager PC are displayed, enter `exit` and check the cable connection.

Applying power to the system

Procedure

1. With the power off on the control unit, insert the B5800 Branch Gateway System SD card into the **System SD** slot on the rear of the control unit.

   Ensure that you have the correct card. The B5800 Branch Gateway System SD card is required for branch operation. The card is labeled **System SD BRANCH GW**.



2. Apply power to the external expansion modules.

   The power outlet used must include a switch and in cases where the power cord includes an earth lead, that outlet must have a protective earth connection.

3. Apply power to the control unit.

   The power outlet used must include a switch and the power outlet must have a protective earth connection.

   When power is applied to the control unit, the following occurs:

   - The control unit begins loading firmware from the System SD card with which it will upgrade itself and the components installed in the control unit. This process takes approximately a minute. The end of this process is indicated by LED1 on each base card flashing every 5 seconds and LED9 on each base card fitted with a trunk daughter card flashing every 5 seconds.

- The control unit will then begin upgrading the external expansion modules. This is indicated by the red center LED on each module flashing red. The process is completed when the LED changes to steady green.
- If a configuration file is already present on the System SD card, it is loaded by the B5800 Branch Gateway. If not, the B5800 Branch Gateway creates a default configuration based on the components of the system and copies that configuration onto the System SD card.

The B5800 Branch Gateway Initial Installation utility is launched. See Using the Initial Installation Utility on page 121.

Control unit LEDs startup sequence

The LEDs on the rear of the control unit go through the following sequence during a normal start up. Note that the times are approximate only.

LED	4s	4s	12s	5s	2s	5s	5s	10s	10s	Finished
CPU	Orng	Grn	Grn	Grn Red	Grn	Grn	Grn	Grn	Grn	Grn
System SD	Orng	Off	Grn	Grn	Grn	Off	Grn	Grn	Grn Flash	Grn
Optional SD (if present)	Orng	Off	Grn	Grn	Grn	Off	Off	Grn	Grn	Grn

Orng = Orange Grn = Green

On the front of the control unit, LED1 on any IP500 base cards fitted is used as follows. LED9 is also used for any trunk daughter cards fitted.

LED	30s	30s	Finished
Optional SD	Red	Red	Red
		Fast Flash	Flash every 5 seconds

About the LEDs

Control unit LEDs

LED	Description
Optional SD	• Off = card shutdown • Green on = card present • Green flashing = card in use • Orange steady = reset imminent • Red flashing = card initializing or shutting down • Red fast flashing = card full • Red steady = card failure/wrong type
System SD	
CPU	• Alternate red/green = starting up • Green on = okay • Red on = no software • Flashing Red = error/shutdown

Base card LEDs

Base Card	LEDs 1 to 8 Usage
All cards	LED1 is used for base card status: • Red on = error • Red slow flash = initializing • Red flash every 5 seconds = card okay • Red fast flash = system shutdown
Analog phone	No status LEDs are used for analog phone extensions.
Digital station	Green on = phone detected
VCM	LEDs 1 to 8 are unlabelled. They are used to indicate voice compression channel usage. Each LED lit represents 12.5% of the available voice compression channel capacity in use (total card capacity rather than licensed capacity).
4-port expansion	LEDs 1 to 8 are used for the expansion ports on the rear of the control unit. LEDs 9 to 12 are used for the card's own expansion ports.

Base Card	LEDs 1 to 8 Usage
	• Green on = expansion module present • Red flashing = initializing • Red on = error • Orange regular flash = base card okay
Combination	LEDs 1 to 6 Green on = phone detected

Trunk daughter card LEDs

Trunk Daughter Card	LEDs 9 to 12 Usage
All cards	LED 9 is used for daughter card status: • Red on = error • Red slow flash = initializing • Red flash every 5 seconds = card okay • Red fast flash = system shutdown
Analog trunk	• Green on =card fitted • Green flashing = trunk in use
BRI trunk	• Off = no trunk present • Green on = trunk present • Green flashing = trunk in use
PRI trunk	• Off = no trunk present • Green on = trunk present • Green flashing = trunk in use • Red/green fast flash (port 9) or greenfast flash (port 10) = alarm indication signal (AIS) from the trunk remote end • Red with green blink (port 9) or green blink (port 10): port in loopback mode (set through System Monitor)

External expansion module LEDs

External expansion module	
All modules	• Green on = module okay • Red flashing = module starting up • Red on = error

Default configuration

Unless you loaded a configuration file onto the System SD card, the B5800 Branch Gateway system will be configured with default settings when the system is started.

Following are the basic default configuration settings for a B5800 Branch Gateway system.

Network Settings	LAN1	LAN2/WAN
IP address	192.168.42.1	192.168.43.1
IP mask	255.255.255.0	255.255.255.0
DHCP mode	server	server
Number of DHCP IP addresses	200	200

- **Extensions and users** — An extension is automatically created for each physical extension port detected in the system. Extension numbers start from 201 and take the form Extn201, Extn202, etc. You must manually configure a user for each extension. Users are not created automatically. Note that there can be extensions on the system that have not yet had users assigned to them.
- **Hunt group** — A single hunt group 200 called Main is created and the first 10 users are placed into that hunt group as members.
- **Incoming call routes** — Two default incoming call routes are created. Voice calls are routed to the hunt group Main. Data calls are routed to the RAS user DialIn.
- **Default short codes** — A-Law or U-Law variant operation is determined by the Feature Key installed in the control unit. Depending on the variant, different short codes and trunk settings are added to the default configuration.
- **A-Law or Mu-Law** — Pulse Code Modulation (PCM) is a method for encoding voice as data. In telephony, two methods of PCM encoding are widely used, A-law and Mu-law (also called U-law). Typically Mu-law is used in North America and a few other locations while A-law is used by the rest of the world. As well as setting the correct PCM encoding for the region, the A-Law or Mu-Law setting of a B5800 Branch Gateway system when it is first started affects a wide range of regional defaults relating to line settings and other

values. The encoding default is set by the type of Feature Key installed when the system is first started.

Default DHCP/IP address settings

When a defaulted or new B5800 Branch Gateway control unit is switched on, it requests IP address information from a DHCP server on the network. This operation will occur whether the LAN cable is plugged in or not. The process below is done separately for both the LAN port (LAN1 in the configuration) and the WAN port (LAN2 in the configuration) on the back of the control unit.

- The B5800 Branch Gateway makes a DHCP request for what IP address information it should use.
- If a DHCP server responds within approximately 10 seconds, the control unit defaults to being a DHCP client and uses the IP address information supplied by the DHCP server.

Note:

For this installation, we have not yet connected the control unit to the network so a DHCP server will not respond.

- If a DHCP server does not respond, the control unit defaults to being the DHCP server for the LAN using the following settings:
  - For its LAN1 it allocates the IP address 192.168.42.1 and IP Mask 255.255.255.0. It supports 200 DHCP clients using the addresses range 192.168.42.2 and 192.168.42.201, the IP Mask 255.255.255.0 and default gateway address 192.168.42.1 (the control unit LAN1 address).
  - For its LAN2 if supported, it allocates the IP address 192.168.43.1 and IP Mask 255.255.255.0.
  - Note that the B5800 Branch Gateway does not check that these addresses are valid and or available on the network.

Important:

Once the control unit has obtained IP address and DHCP mode settings, it retains those settings even if rebooted without a configuration file present on the System SD card. To fully remove the existing IP address and DHCP mode setting the B5800 Branch Gateway must be defaulted using Manager.

Connecting the control unit to the network

Before you begin

The system default settings must be changed to match the customer requirements before the control unit is connected to the network. Use the Initial Installation Utility to assist in configuring the system settings. To run the Initial Installation Utility, see Using the Initial Installation Utility on page 121.

The Initial Installation Utility is run using IP Office Manager from a PC or laptop that is connected directly to the B5800 Branch Gateway LAN 1 port. The Initial Installation Utility will

automatically detect the B5800 Branch Gateway and connect regardless of the PC or B5800 Branch Gateway LAN settings. This utility can be run on site or while the B5800 Branch Gateway control unit is being staged off site.

Note:

IP Office Manager preferences must be set to:

- UDP discovery and 255.255.255.255 (**File > Preferences > Discovery** tab)
- Auto Connect on start up (**File > Preferences > Preferences** tab)

About this task

Once you have changed the B5800 Branch Gateway system default settings to those that match the customer requirements, use this task to connect the B5800 Branch Gateway control unit to the customer's network.

Procedure

1. Disconnect the LAN cable from the installer PC.
2. Connect the LAN cable to the customer network.
3. If you want to use the administration PC for on-going administration, connect the PC to the customer network.

Connecting phones

Procedure

1. Connect the analog phones to the phone ports.
2. Ensure that the analog phones that are connected to power failure ports are clearly labeled as such.
3. Connect the Avaya digital phones to the appropriate DS ports.
   When the control unit is started, after loading its own firmware and the firmware for its external expansion modules, it will upload the appropriate firmware to the digital phones.

   Avaya H.323 phones do not need to be connected at this stage. They will go through a firmware upgrade process when connected to a B5800 Branch Gateway system that is already running.

Chapter 5: Upgrading an R6.1 system to R6.2

This chapter provides the procedures to upgrade a B5800 Branch Gateway deployed in the distributed branch user model from R6.1 to R6.2.

The procedures in this chapter are performed using both IP Office Manager that is connected directly to the B5800 Branch Gateway system and Avaya Aura® System Manager where some procedures are performed from the System Manager Web console.

Upgrade installation checklist

Use this checklist to monitor your progress as you upgrade an R6.1 B5800 Branch Gateway system to an R6.2 system.

#	Description	Section	✔
1	Confirm that your version of Avaya Aura® System Manager is R6.2 and SP1 has been installed.		
2	Create a backup of each B5800 Branch Gateway.	See Creating a backup of the system configuration using IP Office Manager on page 215.	
3	Upgrade the B5800 Branch Gateway. The upgrade wizard upgrades all of the B5800 Branch Gateway components including the modules, cards, and phone firmware.	See Using the upgrade wizard on page 217.	
4	Upgrade the administration applications.	See Upgrading the administration applications on page 90.	
5	Export users to an xml file. **Note:** Be sure to perform this task before you launch the Initial Installation Utility. After you launch the Initial Installation	See Exporting users to an xml file on page 92.	

#	Description	Section	✔
	Utility, the System Manager administration feature for the branch is enabled and the users on the B5800 Branch Gateway are deleted so they will not be available for export.		
6	Edit fields in the xml file so that the data matches the requirements for the corresponding fields in System Manager.	See Editing the xml file containing the users on page 92.	
7	Launch the Initial Installation Utility.	See Using the Initial Installation Utility on page 121.	
8	Add the B5800 Branch Gateways to System Manager.	See About adding B5800 Branch Gateways to System Manager on page 125.	
9	Import users from B5800 Branch Gateway to Avaya Aura® System Manager.	See Bulk importing of users on page 93.	
10	Upgrade the auto attendant greeting files.	See Uploading an auto attendant audio file on page 132.	

Upgrading the administration applications

About this task

Use this procedure to upgrade the B5800 Branch Gateway administration applications from R6.1 to R6.2. The B5800 Branch Gateway administration applications are Manager, System Status, and System Monitor. For more information about the administration applications, see Administration software suite on page 77.

Procedure

1. Using the **Add or Remove Programs** option in the Windows Control Panel, check that the PC does not have an earlier version of the B5800 Branch Gateway Administration Suite installed. It there is, uninstall it.
2. Insert the B5800 Branch Gateway R6.2 Administrator Applications DVD.
3. Select B5800 Branch Gateway Administration Suite.
4. Double-click on **setup.exe**.
5. Select the language you want to use for the installation process.
   This does not affect the language used by Manager when running.

6. Click **Next**.
7. Select who should be able to run the Administration Suite applications.
8. Click **Next**.
9. If required, select the destination to which the applications should be installed. It is recommended that you accept the default destination.
10. Click **Next**.
    The Custom Setup window appears.
11. Select the applications that you want to install. At a minimum select **System Monitor** and **Manager**.
    When you select an application, a description of the application appears. Click on the ▾ next to each application to change the installation selection.
12. Click **Next**.
13. Click **Install**.
    Installation of Windows .Net2 components may be required. If dialogs for this appear, follow the prompts to install .Net.
14. If requested, reboot the PC.

Enabling secure communication after upgrading IP Office Manager

About this task

If an older version of IP Office Manager is installed and you cannot connect to the B5800 Branch Gateway after IP Office Manager has been upgraded, you must enable the secure communication feature in IP Office Manager.

Procedure

1. Start IP Office Manager.
2. Select **File > Preferences**.
3. Click the **Security** tab.
4. Click the **Secure Communications** check box to select this option (check box is checked).
5. Click **OK**.

Exporting users to an xml file

About this task

Be sure to perform this task before you launch the Initial Installation Utility. After you launch the Initial Installation Utility, the System Manager administration feature for the branch is enabled and the users on the B5800 Branch Gateway are deleted so they will not be available for export.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. Select **Tools > Export > Users**.
3. In the **Export Users** dialog box, click the check boxes for the users you want to export.
4. In the **Domain Name** field, enter the appropriate domain name.
5. Browse to the folder where you want to save the .xml file.
6. Click **OK**.
7. In the **Export Users** dialog box, click **OK**.

Editing the xml file containing the users

About this task

Use this task to edit several fields in the xml file so that the data matches the requirements for the corresponding fields in System Manager.

Procedure

1. Using a text editor, open the xml file that contains the exported users.
2. Edit the following fields to match the System Manager field constraints:
   a. Edit the field **<csm:deviceName>***name of device as added on System Manager*<**/csm:deviceName>** to match the Managed Element name of the device as it was added in System Manager.

      This field is exported as the System name field in the B5800 Branch Gateway configuration so it must be changed to match the Managed Element name of the device in System Manager.

b. If the **<givenName>** field does not contain an entry, edit the field **<givenName>***first name***</givenName>** where *first name* is the user's first name.

Note:

The entry for this field is derived from the **Full Name** field that is configured when a user is added to the system. The **Full Name** field is configured in IP Office Manager under **User > User** tab. If the **Full Name** field was not completed when the user was added to the system, the **<givenName>** field for the user will be blank when the user is exported to the xml file. The **<givenName>** field must contain a value. Do not use punctuation characters such as **#**, **?**, **/**, or **,**. Do not begin the entry with a space.

c. Edit the field **<loginName>***login name for the user***</loginName>** where *login name for the user* is in the format *loginname@somedomain.com*, for example **Extn5411000@avaya.com**.

d. If the **<surname>** field does not contain an entry, edit the field **<surname>***last name***</surname>** where *last name* is the user's last name.

Note:

The entry for this field is derived from the **Full Name** field that is configured when a user is added to the system. The **Full Name** field is configured in IP Office Manager under **User > User** tab. If the **Full Name** field was not completed when the user was added to the system, the **<surname>** field for the user will be blank when the user is exported to the xml file. The **<surname>** field must contain a value. Do not use punctuation characters such as **#**, **?**, **/**, or **,**. Do not begin the entry with a space.

e. Edit the field **<userPassword>***password for the user***</userPassword>** so that the password complies with the System Manager user password constraints. The System Manager user password cannot be only numeric. This is the password used to log into System Manager.

3. Save and close the xml file.

Bulk importing of users

Procedure

1. From the System Manager console, under **Services**, select **Bulk Import and Export**.
2. Click **Import > User Management > Users**.
3. On the Import users page, in the **Select File** field, enter the complete path of the file.

Also, you can click **Browse** to locate and select a file.

4. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
5. Select **Complete** as the import type.
6. Select one of the following import options:
   - To skip users in the import file that match the existing user records in the database, click **Skip**.
   - To update and merge the user attributes data from the imported file to the existing data, click **Merge**.
   - To replace the users in the database with the new users from the imported file, click **Replace**. Use this option to import new users and retain the existing users.
   - To delete the user records in the database that match the records in the imported file, click **Delete**.
7. To run the job, in the **Job Schedule** section, select one of the following options:
   - To import the users immediately, click **Run immediately**.
   - To import the users at a specified time, click **Schedule later**, and set the date and time.
8. Click **Import**.

Note:

The operations, Communication Manager Synchronization and Bulk Import of users, must not overlap in time. If Bulk Import of users is in progress and Communication Manager Synchronization is started, the current records under process fail. After the synchronization is complete, the remaining bulk import records process successfully. You must reimport the records that fail during synchronization.

About migrating individual PLDS license files to a WebLM server

After you upgrade the B5800 Branch Gateway R6.1 system to R6.2, you can migrate the individual PLDS license files to the System Manager WebLM server. This requires that you first move the individual PLDS license files from one license host to another license host (that is, from the B5800 Branch Gateway to the System Manager WebLM server) and then install

the shared license file on the System Manager WebLM server. To perform these procedures, see:

- Moving activated license entitlements on page 195. In this procedure you will move the activated license entitlements from the current host ID, which is the individual B5800 Branch Gateway, to the host ID of the WebLM server.
- Enabling WebLM licensing for the branch on page 130
- Installing the shared PLDS license file on the System Manager WebLM server on page 117
- Deleting the PLDS license file from the branch on page 95

Deleting the PLDS license file from the branch

About this task

After the license entitlements in PLDS have been moved from the individual B5800 Branch Gateway license file to the shared WebLM license file, the individual license file installed on each B5800 Branch Gateway must be deleted.

Note:

Failure to delete the individual license file on the B5800 Branch Gateway will create a violation of the end user license agreement.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. Select **File > Advanced > Embedded File Management**.
3. Do the following:
   a. Select the first B5800 Branch Gateway system.
   b. Right-click the file name **PLDSkeys.xml**.
   c. Click **Delete**.
4. Repeat Step 3 for each branch.

Chapter 6: Upgrading an R6.2 system with an R6.2 service pack

This chapter is for B5800 Branch Gateway systems that have already been upgraded from R6.1 to R6.2. Avaya periodically releases service packs to provide updates that fix existing problems or provide enhancements.

This chapter describes how to perform an upgrade using Avaya Aura® System Manager. Avaya Aura® System Manager should be used on R6.2 systems when multiple branches require upgrades.

Two other methods which require using IP Office Manager that is connected directly to the B5800 Branch Gateway system are available to perform an upgrade. You can perform an upgrade using the IP Office Manager upgrade wizard or using the System SD card. For more information, see:

- Using the upgrade wizard on page 217
- System upgrade using the System SD card on page 256

R6.2 service pack installation checklist

#	Description	Section	✔
1	Create a backup of the system configuration.	See Creating a backup of the system configuration using System Manager on page 215.	
2	Synchronize the B5800 Branch Gateway with System Manager.	See Synchronizing B5800 Branch Gateway with System Manager on page 162.	
3	Set up an external server to act as a remote software library.	See Remote Software Library for B5800 Branch Gateway upgrades on page 98.	
4	Get the inventory.	See Getting inventory on page 100.	
5	Configure PLDS access.	See Configuring user PLDS access on page 101.	
6	Create a software library.	See Creating a software library on page 102.	
7	Upgrade the B5800 Branch Gateway.	See Upgrading the B5800 Branch Gateway using System Manager on page 103.	

Remote Software Library for B5800 Branch Gateway upgrades

For the B5800 Branch Gateway firmware upgrade files, an external server is required to act as a remote software library. This server hosts the firmware upgrade files through HTTP. The external server should have an FTP, SCP, or SFTP server to upload the firmware files from System Manager. While downloading from the PLDS web site, the firmware files are temporarily copied on System Manager. The FTP, SCP, or SFTP protocols are then used to copy the firmware files from System Manager to the external server. This file transfer from PLDS to System Manager and then to the external server is a single operation for the administrator.

Note:

The HTTPS protocol is not supported for a B5800 Branch Gateway device to pull files from the external server.

Downloading the firmware files from PLDS to the B5800 elements through System Manager

1. Download the B5800 firmware from PLDS to the System Manager cache using the credentials provided in **User Settings** in System Manager.
2. Upload the firmware to the external server from the System Manager cache using the FTP or SCP or SFTP protocol and the configuration information in the software library.
3. After the file is on the external server, B5800 elements use this file during upgrade using HTTP protocol.

Note:

Steps 1 and 2 happen simultaneously. The file download to System Manager is transparent.

System requirements for the external server

Component	Requirement	Recommendation
Operating System	Any standalone or virtualized Windows or Linux Distribution.	

Component	Requirement	Recommendation
Hard Drive	20GB free space	There should be enough free space on the hard drive to store the firmware files.
Memory	2GB	As required by the operating system and the supported protocol services.
Protocols (for the B5800 Branch Gateway elements to download files from the external server)	HTTP server	Any supported HTTP server installation. **Note:** The HTTPS protocol is not supported for a B5800 Branch Gateway device to pull files from the external server.
Protocols (for downloading the firmware upgrade files to the external server from the PLDS web site via System Manager)	An FTP, SCP or SFTP server (running on default ports)	Use SFTP or SCP for secure file transfer.

Setting up the external server to work as a remote software library for B5800 upgrades

Procedure

1. Install the operating system.
2. Install any supported HTTP server.
3. Install any one of the supported servers: FTP, SFTP, or SCP.
4. Configure users for the FTP or SFTP or SCP access. These users should have read, write, and delete permissions for the directories configured to function as the storage location for the upgrade files.
5. Configure the HTTP server such that the location where the upgrade files are downloaded is accessible using an HTTP URL. This URL is used to configure the external server as a software library on System Manager. As B5800 elements use this HTTPS URL to pull the firmware files during upgrade, the URL must be reachable to the B5800 elements.

Getting inventory

Before you begin

Ensure that all B5800 Branch Gateway devices have been added to System Manager. There are several methods available to add the B5800 Branch Gateways to System Manager. All methods require that you identify each individual B5800 Branch Gateway. See About adding B5800 Branch Gateways to System Manager on page 125 for more information.

The B5800 Branch Gateway devices to be discovered for upgrades should be SNMP enabled and the corresponding SNMPv1 communities must be set correctly in System Manager. See Setting B5800 Branch Gateway SNMP attributes on page 100 for more information.

About this task

Use this task to collect the components of a B5800 Branch Gateway that has been added on System Manager.

Note:

This task does not automatically find the new B5800 Branch Gateways. The B5800 Branch Gateway must first be added to System Manager. Then this task will collect the components for the B5800 Branch Gateway that was added to System Manager.

B5800 Branch Gateways that are added to System Manager using the discovery method described in Discovering B5800 Branch Gateways on page 126 already have their inventory details collected. You do not need to perform this task to upgrade those B5800 Branch Gateways.

Procedure

1. From the System Manager console, under **Elements**, click **Inventory**.
2. On the **Inventory** page, on the left navigation pane, click **Upgrade Management > Manage Software**.
3. On the **Manage Software** page, click **Get Inventory**.
4. Do one of the following:
   - Click **Now** to get the device inventory.
   - Click **Schedule** to get the device inventory at a later time.

Setting B5800 Branch Gateway SNMP attributes

Procedure

1. From the System Manager console, under **Elements**, click **Inventory**.

2. On the **Inventory** page, on the left navigation pane, click **Manage Elements**.
3. Click the check box for the appropriate element.
4. Click **Edit**.
5. On the **Edit <*system name*>** page, click the **Attributes** tab.
6. In the **SNMP Attribute**s section, do the following:
   a. For the **Version**, click the radio button for **V1**.
   b. In the **Read Community** field, enter the read community of the device.
   c. In the **Write Community** field, enter the write community of the device.
   d. In the **Retries** field, select the appropriate number of times the application should poll the device without receiving a response before timing out.
   e. In the **Timeout (ms)** field, select the appropriate number of milliseconds that the application should poll the device without receiving a response before timing out.
   f. In the **Device Type** drop-down box, select the appropriate device type.
7. Click **Commit**.

Configuring user PLDS access

About this task

Use this procedure to configure user PLDS access and define the default support site.

Procedure

1. From the System Manager console, under **Elements**, click **Inventory**.
2. On the **Inventory** page, click **Upgrade Management > User Settings**.
3. On the **User Settings** page, click **Edit**.
4. For the **Use Avaya Support Site** check box, accept the default setting, checked.

   Note:

   Use **Other Website** only if a service technician directs you to use an alternate site for downloads.
5. In the **SSO User Name** field, enter the user's SSO user name for PLDS.
6. In the **SSO Password** field, enter the user's SSO password for PLDS.
7. Click the **Use Proxy** check box if the user has a proxy.
8. In the **Host** field, enter the host details for this proxy server.
9. In the **Port** field, enter the port number for this proxy server.

10. Click **Commit**.

Creating a software library

Procedure

1. From the System Manager console, under **Elements**, select **Inventory**.
2. On the **Inventory** page, click **Upgrade Management > Software Library**.
3. Click **New**.
4. On the **Add Software Library** page, in the **Library Server Details** tab, do the following:
   a. In the **Name** field, enter the appropriate name.
   b. In the **IP Address** field, enter the IP address of the library server.
   c. In the **Description** field, enter a description of this library server as appropriate.
   d. In the **Server Path** field, enter the full path of the software library location
   e. To use this software library as the default, click the **Default Library** check box.
   f. If this software library is remote, click the **Remote Library** check box.
   g. In the **Default Protocol** drop-down box, select the appropriate protocol.
   h. Click the **HTTP/HTTS** check box.
   i. In the **HTTP/HTTS URL** field, enter the appropriate URL to the firmware files in **Software Library**.
   j. Depending on the default protocol you selected in step g, click on the corresponding tab (**FTP Configuration**, **SCP Configuration**, or **SFTP Configuration**) and configure the authentication parameters as required.

      Note:

      Configuring the authentication parameters for the default protocol is mandatory.
   k. Click **Commit**.

Upgrading the B5800 Branch Gateway using System Manager

About this task

Use this task to upgrade the B5800 Branch Gateway. Included in this task are the steps to:

- analyze the software to determine if a new version is available
- download the firmware files from Avaya PLDS

Avaya PLDS will automatically determine if a newer software version than what is currently installed is available. If there is a newer version available, you can download the newer version to upgrade the B5800 Branch Gateway. To determine if there is a new software version available, Avaya PLDS uses the file *versions_sp.xml* that is available from the Avaya Support Site to compare the current installed software on the device with the latest available on Avaya PLDS. The file *versions_sp.xml* is regularly updated with the latest firmware/software releases available for upgrade.

Procedure

1. From the System Manager console, under **Elements**, select **Inventory**.
2. On the **Inventory** page, click **Upgrade Management > Manage Software**.
3. On the **Manage Software** page, click **More Actions > Analyze Now**.
4. When the analyze job is finished running, refresh the table.
   A red **x** indicates there is a newer firmware version available that has not been downloaded to the software library.
5. Select the control unit for upgrade, and click **Download**.
6. On the **File Download Manager** page, do the following:
   a. In the **Library** drop-down box, select the appropriate library.
   b. In the **Protocol** drop-down box, accept the protocol displayed.

      Note:

      The appropriate protocol is automatically selected based on the selected library.
   c. Expand the tree to show a list of the upgrade packages that are available.
   d. Under the Device Type **B5800**, select the latest package.
7. Do one of the following:
   - Click **Now** to download the software.
   - Click **Later** to schedule the download at a specified time.
8. Click **Download**.

The system displays the End User License Agreement page.

9. Click **Accept** to download the software.
10. When the download is complete, go to the **Manage Software** page.

    A yellow `i` indicates there is a newer version of software downloaded to the remote software library and the device can be upgraded.
11. Click the check box for the appropriate control unit.
12. Click **Upgrade**.

    The **Upgrade** button is enabled only if the state of the device is yellow.
13. On the **B5800 Branch Gateway Upgrade Configuration** page, select the appropriate library and the release to which you want to upgrade.

    By default, the library which has the latest upgrade package is automatically selected.
14. Do one of the following:

    - Click **Now** to start the upgrade.
    - Click **Later** to schedule the upgrade at a specified time.
15. To view the upgrade status, on the **Manage Software** page, click the B5800 Branch Gateway being upgraded, then click **Status**.
    When the upgrade is complete, a final status window is displayed. The state of the device turns green showing that it has the latest firmware installed.

Chapter 7: Administration software suite

The IP Office administration software applications are installed on the installation PC. They are used by installers and maintainers to configure, manage, and monitor the B5800 Branch Gateway system.

The IP Office administration applications are:

- **Manager**

  IP Office Manager is used to access all parts of the B5800 Branch Gateway configuration. Different levels of access can be defined to control which parts of the configuration the Manager user can view and alter. Manager is also used to upgrade the system software files.

- **System Status**

  The IP Office System Status application is a monitoring and reporting tool that provides a wide range of information about the current status of the system. It can report the available resources and components within the system and details of calls in progress. Details of the number of alarms are recorded and the time and date of the most recent alarms.

- **System Monitor**

  The IP Office System Monitor application is a tool that shows details of all activity on the B5800 Branch Gateway system. Because of the level of detail, interpretation of System Monitor traces requires a high-level of data and telephony protocol knowledge. Installers and maintainers must understand how to run System Monitor when necessary as Avaya may request copies of System Monitor traces to resolve support issues.

Starting System Status

About this task

The IP Office System Status application is a monitoring and reporting tool that provides a wide range of information about the current status of the system. It can report the available resources and components within the system and details of calls in progress. Details of the number of alarms are recorded and the time and date of the most recent alarms.

Procedure

1. To start the System Status application, choose one of the following:
   - On the PC where System Status has been installed, select **Start** > **Programs** > **Avaya B5800 Branch Gateway Admin Suite** > **System Status**.

- If Manager is also installed and is running, select **File** > **Advanced** > **System Status**.
- Start a web browser and enter the IP address of the B5800 Branch Gateway control unit. Then select the System Status Application link.

The Logon window appears.

2. In the Logon window, enter the details of the B5800 Branch Gateway system to which you want it to connect as follows:
   a. In the **Control Unit IP Address** drop-down box, select the appropriate address, or enter the IP address of the control unit.
   b. In the **Services Base TCP Port** field, enter the Services Base TCP Port setting that was set in the system's security settings. The default is 50804
   c. In the **Local IP Address** field, enter the appropriate local IP address. If the PC has more than one IP address assigned to its network card or multiple network cards, the address to use can be selected if necessary.
   d. In the **User Name** field, enter a user name that has been configured for System Status access in the B5800 Branch Gateway security settings.
   e. In the **Password** field, enter the appropriate password.
   f. Check the **Auto Reconnect** check box if you want System Status to attempt to reconnect using the same settings if connection to the B5800 Branch Gateway is lost.
3. Click **Logon**.

Starting System Monitor

About this task

The IP Office System Monitor application is a tool that shows details of all activity on the B5800 Branch Gateway system. Because of the level of detail, interpretation of System Monitor traces requires a high-level of data and telephony protocol knowledge. Installers and maintainers must understand how to run System Monitor when necessary as Avaya may request copies of System Monitor traces to resolve support issues.

Procedure

1. Select **Start** > **Programs** > **Avaya B5800 Branch Gateway Admin Suite** > **Monitor**.
   If System Monitor has been run before it will attempt to connect with the system which it monitored previously.
2. To monitor a different system, select **File** > **Select Unit**.
   The Select System to Monitor window appears.

3. In the Control Unit IP Address drop-down box, select the IP address of the control unit you want to monitor.
4. In the Password field, enter the appropriate password.

   Note:

   You are able to set a System Monitor password using Manager. If the B5800 Branch Gateway does not have a System Monitor password set, System Monitor uses the B5800 Branch Gateway System password. The System Monitor password and System password are both set within the B5800 Branch Gateway system security settings.
5. For Control Unit Type, select **Avaya B5800 Branch Gateway**.
6. Click **OK**.

Chapter 8: Initial branch configuration

This chapter provides initial configuration tasks required for each B5800 Branch Gateway deployed in the distributed branch user model.

Configuration checklist

Use this checklist to monitor your progress as you configure a B5800 Branch Gateway system deployed as a distributed branch.

#	Description	Section	✔
1	Confirm that your version of Avaya Aura® System Manager is R6.2 and SP1 has been installed.		
2	Download IP Office Manager onto the System Manager server.	See Setting up System Manager to launch IP Office Manager on page 112. **Note:** This task is not required if you have downloaded the B5800AdminLite.exe file using the Upgrade Management link in System Manager.	
3	Install the shared PLDS license file on the System Manager WebLM server.	See Installing the shared PLDS license file on the System Manager WebLM server on page 117. **Note:** If you are using the individual licensing method, see Using Manager to deliver license files to the branches on page 117.	
	Note: Steps 1 through 3 only need to be performed one time. They do not need to be performed for each new B5800 Branch Gateway.		
4	Generate a certificate on Avaya Aura® System Manager.	See Generating a certificate on System Manager on page 119.	

#	Description	Section	✔
5	Run the Initial Installation Utility. The Initial Installation utility provides configuration and security settings that minimize initial installation activities and maximize security.	See Using the Initial Installation Utility on page 121. **Note:** When you run the Initial Installation Utility, a security certificate is automatically installed on the B5800 Branch Gateway. If you do not run the Initial Installation Utility, you must manually configure the SCEP and security settings on the B5800 Branch Gateway. This is not the preferred method, but can be used as an alternative. For more information, see Configuring the B5800 Branch Gateway for certificates on page 123.	
6	Add the B5800 Branch Gateways to System Manager.	See Discovering B5800 Branch Gateways on page 126. In this task, you add the branch to System Manager by identifying the subnet IP address in which the branch is located. This task must be performed for each B5800 Branch Gateway that you want to manage from System Manager. As an alternative, you can also use one of the following methods to add the B5800 Branch Gateways to System Manager: • Bulk importing of devices on page 128. This method requires that you first add each B5800 Branch Gateway to an xml file. The xml file is then used to import the devices to System Manager. • Adding the B5800 Branch Gateways to System Manager on page 129. In this task, you manually add each branch to System Manager by identifying the IP address of the B5800 Branch Gateway. This task must be performed for each B5800 Branch Gateway that you want to manage from System Manager.	
7	Confirm that WebLM licensing for the branch is enabled.	See Enabling WebLM licensing for the branch on page 130.	
8	Create a system template. (Optional)	See Creating a system template on page 131.	

#	Description	Section	✔
9	Uploading an auto attendant audio file. (Optional)	See Uploading an auto attendant audio file on page 132.	
10	Apply the system template to one or more branches. (Optional)	See Applying the system template on page 132.	
11	Create an endpoint template.	See Creating an endpoint template on page 133. **Note:** You must create a B5800 Branch Gateway endpoint template. You cannot add a user in System Manager unless an endpoint template has been created.	
	Note: • Steps 12 through 23 are performed to modify a B5800 Branch Gateway configuration as needed. • Steps 24 through 12 are performed to configure Avaya Aura®Session Manager. • Step 32 is performed to configure B5800 Branch Gateway users from User Management within System Manager.		
12	Disable unused trunks.	See Disabling unused trunks on page 134.	
13	Set a trunk clock quality setting.	See Setting a trunk clock quality setting on page 136.	
14	Set trunk prefixes.	See Setting the trunk prefixes on page 137.	
15	Enable SIP trunk support.	See Enabling SIP trunk support on page 139.	
16	Set the branch prefix and local number length for the extension numbering.	See Setting the branch prefix and local number length for extension numbering on page 140.	
17	Change the default codec selection.	See Changing the default codec selection on page 143.	
18	Change the maximum SIP sessions.	See Changing the maximum SIP sessions on page 144.	
19	Add a Session Manager line.	See Adding an Avaya Aura Session Manager line on page 145. This procedure includes the steps to configure TLS transport for the Session Manager line.	

#	Description	Section	✔
20	Add a second Session Manager line for redundancy.	See Avaya Aura Session Manager line redundancy on page 150.	
21	Set up outgoing call routing.	• See Setting up outgoing call routing on page 151. • For information on routing back to the branch for fallback alternate routes, see Branch PSTN call routing examples on page 289.	
22	Configure the type of voicemail system the branch will use.	See Voicemail options on page 171.	
23	Enable branch SIP extension support.	See Enabling branch SIP extension support on page 154.	
	Note: Steps 24 through 31 are performed to configure Avaya Aura® Session Manager.		
24	View a list of the SIP domains.	See Viewing the SIP domains on page 166.	
25	Create a location.	See Creating locations on page 166.	
26	Create a digit adaptation.	See Creating adaptations on page 167.	
27	Create a SIP entity.	See Creating SIP entities on page 167.	
28	Create an entity link.	See Creating entity links on page 168.	
29	Create a time range.	See Creating time ranges on page 169.	
30	Create a routing policy.	See Creating routing policies on page 169.	
31	Create a dial pattern.	See Creating dial patterns on page 170.	
32	Add distributed users. This task is performed from Avaya Aura® System Manager using the User Management feature.	See User administration on page 185.	

Setting up System Manager to launch IP Office Manager

About this task

From the administration PC, you can use the full version of IP Office Manager available on the B5800 Branch Gateway Administrator Applications DVD or IP Office Manager Lite that is provided in the B5800AdminLite.exe file to view and edit a B5800 Branch Gateway system

configuration or security configuration from System Manager. System Manager launches either version of IP Office Manager in the appropriate mode for the configuration task that was initiated, such as endpoint or template configuration.

If you use IP Office Manager that was installed from the B5800 Branch Gateway Administrator Applications DVD, you must ensure the version installed on the administration PC is the same version in the B5800AdminLite.exe file. If they are not the same version, you must either upgrade the version of IP Office Manager on the administration PC or you must update the version of IP Office Manager in the System Manager file. To update the version in the System Manager file, update the parameter **abg_b5800_mgr_version** in the file **`/opt/Avaya/ABG/tools/ManagerSFXVersion.properties`** with the version of IP Office Manager that is installed on the administration PC.

To use IP Office Manager Lite to manage the B5800 Branch Gateways, download the B5800AdminLite.exe file to the System Manager server as follows:

Note:

This task is not required if you have downloaded the B5800AdminLite.exe file using the Upgrade Management link in System Manager.

Procedure

1. Download the **B5800AdminLite.exe** file from http://plds.avaya.com.
2. Transfer the downloaded **B5800AdminLite.exe** file to the System Manager server to the directory `/opt/Avaya/ABG/<version>/tools`. For example, `/opt/Avaya/ABG/6.2.12/tools`.

   Use any SCP or SFTP protocol to connect to the server and transfer the file. You may use any client to perform this step.
3. Change this file into an executable file using the command **chmod +x <*file name*>**.
4. Create a soft link using the name **ManagerSFX.exe** for the uploaded file, as follows:
   a. Go to $ABG_HOME/tools by entering `cd $ABG_HOME/tools`.
   b. Use the command **ln –sf <*target*> <*linkname*>** to create the soft link.

      For example, if the file name uploaded to $ABG_HOME/tools is **B5800AdminLite.exe**, then enter `ln –sf B5800AdminLite.exe ManagerSFX.exe`.
5. Using any Linux editor, update the parameter **abg_b5800_mgr_version** in the `/opt/Avaya/ABG/<version>/tools/ManagerSFXVersion.properties` file with the version of IP Office Manager you downloaded from PLDS.

   Important:

   You must update the parameter **abg_b5800_mgr_version** each time you download a new version of IP Office Manager from PLDS and transfer to System Manager. If you fail to do so, when you try to launch IP Office Manager from System Manager, the launch will fail and the system will display an error message prompting you to update the parameter.

6. On the administration PC that will be used to launch IP Office Manager Lite, set the environment variable to match the version of the B5800AdminLite.exe file.

   Depending on the version of Windows running on the PC, do one of the following:

   - If the PC is running Windows 7, go to step 7.
   - If the PC is running Windows XP, go to step 8.

7. If the PC is running Windows 7, do the following:
   a. From the Start menu, right-click **Computer**.
   b. Click **Properties**.
   c. In the left navigation pane, click **Advanced system settings**.
   d. In the **System Properties** dialog box, click **Environment Variables**.
   e. In the **Environment Variable** dialog box, in the **User variables for *<name>*** area, select **AVAYAB5800_VER**.
   f. Click **Edit**.
   g. In the **Edit User Variables** dialog box, in the **Variable value** field, change the value to match the version of B5800AdminLite, for example, 6.2.
   h. Click **OK**.
   i. Click **OK** for each subsequent dialog box, and then click **Apply**.

8. If the PC is running Windows XP, do the following:
   a. From the Start menu, right-click **My Computer**.
   b. Click **Properties**.
   c. In the **System Properties** dialog box, click the **Advanced** tab.
   d. Click **Environment Variables**.
   e. In the **Environment Variables** dialog box, in the **User variables for *<name>*** area, select **AVAYAB5800_VER**.
   f. Click **Edit**.
   g. In the **Edit User Variable** dialog box, in the **Variable value** field, change the value to match the version of B5800AdminLite, for example, 6.2.
   h. Click **OK**.
   i. Click **OK** for each subsequent dialog box, and then click **Apply**.

9. Install IP Office Manager Lite on the administration PC. See Installing IP Office Manager from the System Manager server to a PC on page 114.

Installing IP Office Manager from the System Manager server to a PC

Before you begin

The B5800AdminLite.exe file has been downloaded to the System Manager server.

About this task

Perform this task to install IP Office Manager from the System Manager server to a PC. Once you perform this task, the next time you attempt to view or edit a B5800 Branch Gateway device from System Manager on this PC, IP Office Manager will automatically launch.

Procedure

1. From the System Manager console, under **Elements**, select **B5800 Branch Gateway**.
2. In the left navigation pane, click **System Configuration**.
3. On the B5800 Branch Gateway System Configuration page, select the B5800 Branch Gateway device whose system configuration you want to view or edit.
4. At the prompt **Do you want to download Avaya B5800 Branch Gateway Manager from the server now?**, click **Yes**.
5. In the **File Download** dialog box, click **Save**.
6. Save the file to an appropriate directory, for example **C:\Program Files\Avaya \B5800**.
7. After the download completes, in the **Download complete** dialog box, click **Run**.
8. In the **Internet Explorer - Security Warning** dialog box where you are prompted **Are you sure you want to run this software?** click **Run**.
9. In the **WinZip Self–Extractor** dialog box where you are prompted **Do you want to install IP Office Manager?** click **Setup**.
10. In the **IP Office Manager Lite – InstallShield Wizard** dialog box, do the following:
    a. In the **Welcome** dialog box, click **Next**.
    b. In the **Customer Information** dialog box, click **Next**.
    c. In the **Destination Folder** dialog box, click **Next**.
    d. In the **Custom Setup** dialog box, click **Next**.
    e. Click **Install**.
    f. In the **InstallShield Wizard Completed** dialog box, click **Finish**.
11. Restart your PC.
12. To verify your PC is configured correctly, select **My Computer > System Properties > Advanced tab > Environment Variables**.

Activating license files

About this task

B5800 Branch Gateway R6.2 uses the Avaya Product Licensing and Delivery System (PLDS) and integration with Web License Manager (WebLM) for B5800 Branch Gateway license

management. B5800 Branch Gateway R6.2 also supports local licensing using an individual PLDS license file that can be installed directly on the B5800 Branch Gateway using B5800 Branch Gateway Manager (provided in R6.1). For more information about both of these licensing methods, see Licensing on page 16.

Note:

B5800 Branch Gateway supports a 30-day grace period during which time the system is fully functional if:

- a license error is detected
- the WebLM server is not available (for example, due to loss of connectivity between the B5800 Branch Gateway and the WebLM server, if using the WebLM licensing method)
- a license file cannot be obtained (for example, due to loss of WAN connectivity, if using the local PLDS licensing method)

Procedure

1. See Activating license entitlements on page 191 to generate the licenses.
2. See one of the following:
   - To use the WebLM licensing method and install the license file on the WebLM server, see Installing the shared PLDS license file on the System Manager WebLM server on page 117.
   - To use the individual PLDS licensing method and install the license file on the B5800 Branch Gateway, see Using Manager to deliver license files to the branches on page 117.

     Note:

     If the B5800 Branch Gateway is centrally managed by System Manager, to install the individual PLDS license file on the B5800 Branch Gateway using Manager, you must first disable the System Manager administration feature for the branch. See Disabling the System Manager administration feature for the branch from System Manager on page 160. After you upload the license file, you must change the B5800 Branch Gateway back to System Manager control by enabling the System Manager administration feature for the branch.

     An alternative method to install the individual PLDS license on a B5800 Branch Gateway that is centrally managed by System Manager is to use the Embedded File Management feature available in B5800 Branch Gateway Manager. You do not need to disable/enabled System Manager administration for the branch using this method. See Using Embedded File Management to install a PLDS license on page 118 for more information.

Installing the shared PLDS license file on the System Manager WebLM server

Before you begin

A shared B5800 Branch Gateway license file has been activated with the Host ID of the WebLM server. See Activating license entitlements on page 191.

Procedure

1. On the System Manager console, under **Services**, click **Licenses**.
2. In the left navigation pane, click **Install License**.
3. Click the **Browse** button and navigate to the appropriate license file.
4. Click the **Install** button.

Using Manager to deliver license files to the branches

Before you begin

License files have been activated with the Host ID (that is, the Feature Key Serial Number) printed on the B5800 Branch Gateway System SD card. See Activating license entitlements on page 191.

About this task

You can use Manager to distribute activated license files to B5800 Branch Gateway sites. This procedure explains how to distribute the license files to a single branch at a time.

If the B5800 Branch Gateway is centrally managed by System Manager, you must first disable the System Manager administration feature for the branch. After you download the license file, you must then enable the System Manager administration feature for the branch. See Disabling the System Manager administration feature for the branch from System Manager on page 160.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, select **PLDS License**.
3. Right-click **PLDS License** and select **Send license file to Avaya Branch Gateway**.
4. In the Upload Files window, select the PLDS license xml file.
   Manager copies the license file to the B5800 Branch Gateway SD card where it is validated and stored for persistent use.

5. Select **File > Close Configuration**.
6. To view the license, select **File > Open Configuration**.

Using Embedded File Management to install a PLDS license

Before you begin

License files have been activated. See Activating license entitlements on page 191.

About this task

Use this procedure to install an individual PLDS license on a B5800 Branch Gateway that is centrally managed by System Manager. To use this feature you must rename the PLDS license file to **PLDStemp.xml**. The B5800 Branch Gateway will validate the **PLDStemp.xml** file, and if the validation succeeds the B5800 Branch Gateway will automatically rename the file to **PLDSkeys.xml** and save it (overriding the previous valid license file, if any was installed).

Note:

When you use Manager to install the license file, you do not need to rename the PLDS license file. The Manager application automatically renames the PLDS license file to **PLDStemp.xml**. See Using Manager to deliver license files to the branches on page 117.

Procedure

1. Start Manager.
2. Select **File > Advanced > Embedded File Management**.
3. In the Select B5800 window, click the check box next to the B5800 Branch Gateway system.
4. Click **OK**.
5. In the B5800 Embedded File Management dialog box, enter the Service User Password.
6. Click **OK**.
7. In the Folders pane on the left, select **System SD > System > Primary**.
8. Select **File > Upload file**.
9. Select the **PLDStemp.xml** file.
10. Click **OK**.
    The Upload System Files window appears and shows the upload progress.
11. When the upload is complete, click **Close**.
12. From the Primary folder, perform a refresh.
    The B5800 Branch Gateway error mode will change to License Normal Mode. The PLDStemp.xml filename is automatically renamed to PLDSkeys.xml.

Note:

If the PLDS file is not accepted by B5800 Branch Gateway, the B5800 Branch Gateway will remain in License Error Mode and the PLDStemp.xml file is not renamed.

Generating a certificate on System Manager

About this task

Use this procedure to add a B5800 Branch Gateway End Entity to System Manager. This procedure adds the B5800 Branch Gateway to the System Manager trust domain and is required to establish a trust relationship between the B5800 Branch Gateway and System Manager.

Procedure

1. From the System Manager console, under **Services**, select **Security**.
2. On the **Security** page, in the left navigation pane, select **Certificates > Authority**.
3. In the left navigation pane, click **Add End Entity**.
4. On the **Add End Entity** page, do the following:
   a. In the **End Entity Profile** drop-down box, select **INBOUND_OUTBOUND_TLS**.
   b. In the **Username** field, enter the name of the B5800 Branch Gateway system.
   c. In the **Password** field, enter a certificate password.

      Note:

      This password will be used as the Simple Certificate Enrollment Protocol (SCEP) password.
   d. In the **Confirm Password** field, enter the password again.
   e. In the **CN, Common Name** field, enter the appropriate name. This name should match the name of the B5800 Branch Gateway system you entered in the **Username** field.

      Note:

      The certificate name cannot contain spaces.
   f. In the **Certificate Profile** drop-down box, accept the default setting, **ID_CLIENT_SERVER**.
   g. In the **CA** drop-down box, accept the default setting, **tmdefaultca**.
   h. In the **Token** drop-down box, accept the default setting, **User Generated**.

i. Click the **Add End Entity** button.
The page refreshes and a message appears at the top of the page stating the End Entity was added successfully.

5. In the left navigation pane, click **List/Edit End Entities**.
6. On the **List/Edit End Entities** page, in the **Or with status** drop-down box, select **All**.
7. Click the **List** button.
8. Confirm the B5800 Branch Gateway End Entity that you just added is listed. Note that **New** appears in the **Status** column for this End Entity. This indicates System Manager has prepared the certificate for exchange with an End Entity.
9. In the left navigation pane, click **Public Web**.
10. On the **Welcome to the public EJBCA** page, in the left navigation pane, click **Create Keystore**.
11. On the **EJBCA Certificate Enrollment** page, in the **Username** field, enter the same username you entered when you created the End Entity in Step 4.
12. In the **Password** field, enter the same password you entered when you created the End Entity in Step 4.
13. Click **OK**.
14. In the **Options** section, accept the default settings for the **Key length** and **Certificate profile** fields, and click **OK**.
The certificate is installed in your browser.
15. In the **Alert** dialog box, click **OK**.
16. From your Firefox browser, to view the certificate, do the following:
    a. Select **Tools > Options**.
    b. In the **Options** window, click **Advanced**.
    c. Click the **Encryption** tab.
    d. Click the **View Certificates** button.
    e. In the **Certificate Management** window, click the **Your Certificates** tab.
17. From your Firefox browser, to save the certificate in the X.509 PEM format, do the following:
    a. In the **Certificate Management** window, click the **View** button.
    b. In the **Certificate Viewer** window, click the **Details** tab.
    c. Click **Export**.
    d. In the **Save Certificate to File** window, in the **Filename** field, change the file name suffix to `.cer`. The .cer format is required for B5800 Branch Gateway.
    e. Click **Save**.

18. If you are not going to use the Initial Installation Utility, go to Configuring the B5800 Branch Gateway for certificates on page 123.

Using the Initial Installation Utility

About this task

The B5800 Branch Gateway Initial Installation utility provides a default configuration and security settings that minimize initial installation activities and maximize security. The system must be configured with the default settings before the system can be administered by Avaya Aura® System Manager. This utility is used for new installations and after an R6.1 to R6.2 upgrade to enable System Manager administration of the B5800 Branch Gateway.

Note:

For new installations, use the Initial Installation Utility before the control unit is connected to the network. See Connecting the control unit to the network on page 86 for more information. The Initial Installation Utility can be used to administer the control unit on site or while the B5800 Branch Gateway control unit is being staged off site.

This procedure includes the steps to manually launch the Initial Installation utility. When a new B5800 Branch Gateway is detected, the Initial Installation utility is launched automatically, so you would begin with Step 3.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. Select **File > Advanced > Launch Initial Installation Utility**.
3. In the **System Name** field, enter the appropriate system name.
4. For the **WAN Interface**, select **LAN1** to connect to the enterprise network.

   Warning:

   You are also able to select LAN2 to connect to the enterprise network. However, LAN2 is primarily intended to connect to the Internet or to public SIP trunks from carriers.

   The LAN2 firewall is normally disabled. If you select LAN2 and choose to enable the firewall, be sure to open the necessary ports for communicating with the enterprise network. For more information, see Avaya port matrix for B5800 Branch Gateway and SIP phones on page 275.
5. In the **IP Address** field, enter the appropriate IP address.
6. In the **IP Mask** field, enter the appropriate IP mask.
7. In the **Gateway** field, enter the appropriate gateway.

IP Office Manager will create an IP route using this gateway with the selected WAN as the destination.

8. In the **DHCP Mode** section, click the radio button for **Disabled**.
9. In the **New Administrator Password** field, enter a new administrator password.
10. In the **New Security Password** field, enter a new security password.

    Note:

    The **New Administrator Password** and **New Security Password** fields appear only when these passwords are set to the default. Once you change the default passwords, the next time you run the Initial Installation Utility, these fields will not appear.

11. If you want the B5800 Branch Gateway to be managed by System Manager, check the **Under Centralized Management?** check box. Then complete the following fields.
    a. In the **SMGR Address** field, enter the IP address of the System Manager server.
    b. In the **SNMP Community** field, enter the appropriate SNMP community. This is the SNMP community for System Manager.

       Note:

       This field must be configured correctly in order for the centralized management functionality to work.
    c. In the **SNMP Device ID** field, enter the alarm ID you receive from a registration.
    d. In the **Trap Community** field, enter the appropriate trap community. This is the SNMP community for the Secure Access Link (SAL) gateway.

       Note:

       This field must be configured correctly in order for the centralized management functionality to work.

       The SNMPv1 trap community string can be set from the System Manager console in under **Services > Configurations > Settings > SMGR > TrapListener**. The trap community string in System Manager should match the trap community string set on the device so that System Manager receives the device alarms properly.
    e. In the **Device Certificate Name** field, enter the appropriate certificate authority name.

       Note:

       The device certificate name cannot contain spaces.
    f. In the **Certificate Enrollment (SCEP) Password** field, enter the appropriate password.

12. Click **Save**.
    The B5800 Branch Gateway reboots.

Result

When the B5800 Branch Gateway is administered by System Manager, the following is automatically configured:

- SNMP enabled
- SNMP trap destination 1 from System Manager IP address
- All SNMP traps active
- WebLM client active
- WebLM service address from System Manager IP address
- Remove all default extension users, leaving “NoUser” and “RemoteManager”

Additional features configured by the Initial Installation Utility

After you run the Initial Installation Utility, the following features are also configured:

- System Status Interface (SSA) service security level – Unsecure only
- Configuration service security level – Secure, Medium
- Security Administration service security level – Secure, Medium
- OAMP Web Services service security level – Secure, Low (if locally administered)
- OAMP Web Services service security level – Secure, High (if administered by System Manager)
- Admin Client Certificate checks:-- High (if administered by System Manager)
- SCEP client active (if administered by System Manager)
- SCEP server IP address from SMGR IP address (if administered by System Manager)
- Legacy Program Code – Active (if locally administered)

Configuring the B5800 Branch Gateway for certificates

Before you begin

Generate a certificate on System Manager. See Generating a certificate on System Manager on page 119.

About this task

Perform this procedure to configure the SCEP and security settings for a B5800 Branch Gateway.

Note:

Perform this procedure only if you did *not* run the Initial Installation Utility. When you run the Initial Installation Utility, the SCEP and security settings are automatically configured for the B5800 Branch Gateway. See Using the Initial Installation Utility on page 121 for more information.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. Select **File** > **Advanced** > **Security Settings**.
3. In the **Select IP Office** window, click the check box for the appropriate system.
4. Click **OK**.
5. In the **Security Service User Login** window, enter a user name and password of an account that has security configuration access to the B5800 Branch Gateway system.

   The defaults are **security** and **securitypwd**.
6. In the **Security Settings** pane, click **System**.
7. Click the **Certificates** tab.
   The certificate settings are set to the default values. The **Issued to** field shows the default certificate that resides on the B5800 Branch Gateway. The default value is the MAC address of the B5800 Branch Gateway system.
8. In the **Identity Certificate** section, click **Delete** to delete the default certificate.
9. In the **Warning** dialog box, click **OK**.
10. In the **Default Certificate Name** box, enter the appropriate name. This is the same name you used when you created the certificate for the End Entity in System Manager. See Generating a certificate on System Manager on page 119 for more information.
11. In the **Received Certificate Checks (Management Interfaces)** drop-down box, accept the default setting, **None**.
12. In the **Received Certificate Checks (Telephony Endpoints)** drop-down box, accept the default setting, **None**.
13. In the **SCEP Settings** section, do the following:
    a. Click the **Active** check box to select that option.
    b. In the **Request Interval (Seconds)** box, accept the default setting, **120**.
    c. In the **SCEP Server IP/Name** field, enter the IP address of the System Manager server. Include `https://` at the beginning of the IP address, for example `https://123.4.567.89`.

d. In the **SCEP Server Port** field, accept the default setting, **443**.
e. In the **SCEP URI** field, accept the default setting.
f. In the **SCEP Password** field, enter the appropriate password. This is the same password you used when you created the certificate for the End Entity in System Manager. See Generating a certificate on System Manager on page 119 for more information.
g. Click **OK**.

14. Click **File > Save** to save the security configuration.
15. From the System Manager console, do the following:
    a. Go to the **List End Entities** page. (See Steps 1 to 2 in Generating a certificate on System Manager on page 119.
    b. In the left navigation pane, click **List End Entities**.
    c. Click the **Reload** button to reload the End Entity.
    After the page refreshes, the status of the End Entity changes from **New** to **Generated**. This indicates the End Entity certificate exchange has occurred.
16. In Manager, return to the **Certificates** tab. See Steps 1 to 7 above.
17. In the **Received Certificate Checks (Management Interfaces)** drop-down box, select **Medium**.
    This ensures the B5800 Branch Gateway will enforce the use of certificates.
18. Click **OK**.
19. Click **File > Save** to save the security configuration.
20. Perform a synchronization. See Synchronizing B5800 Branch Gateway with System Manager on page 162.

About adding B5800 Branch Gateways to System Manager

There are three different methods available that can be used to add B5800 Branch Gateways to System Manager. See one of the following topics:

- Discovering B5800 Branch Gateways on page 126. This method requires you to identify the subnet IP address in which each branch is located. This method does not automatically discover all B5800 Branch Gateways in a network.
- Bulk importing of devices on page 128. This method requires you to manually add each B5800 Branch Gateway to an xml file that is then used for bulk import to System Manager.
- Adding the B5800 Branch Gateways to System Manager on page 129. This method requires you to manually add each branch to System Manager by identifying the IP address of the B5800 Branch Gateway.

Discovering B5800 Branch Gateways

Before you begin

Enable SNMP on the B5800 Branch Gateway to be updated. See Enabling SNMP and polling support on page 127.

About this task

Use this task to discover the B5800 Branch Gateways in the network and add them to System Manager. This task requires that you identify the subnet IP address in which the branch is located. There is always one B5800 Branch Gateway per branch and each branch is in a different subnet. This procedure must be performed for each branch.

Procedure

1. From the System Manager console, under **Elements**, select **Inventory**.
2. On the Inventory page, select **Inventory Management > Configuration**.
3. On the Configuration page, click **New**.
4. On the Add SNMP Access Configuration page, in the **Type** drop-down box, select **V1**.
5. In the **Description** field, enter a description to help identify this SNMP access configuration.
6. Set the **Read Community** field as configured on the device.
7. Set the **Write Community** field as configured on the device.
8. Accept the default settings in the **Timeout (ms)** and **Retries** fields.
9. Click **Commit**.
10. On the Configuration page, click the **Subnets** tab.
11. Click **New**.
12. On the Add Subnet Configuration page, in the **Subnet IP** field, enter the IP address of the subnet in which the branch is located.
13. In the **Subnet Mask** field, enter the subnet mask in which the branch is located.
14. In the **Use SNMP V3** drop-down box, accept the default setting, **No**.
15. Under **SNMP Access**, click the check box(es) to select the appropriate SNMP access configuration(s).
16. Click **Commit**.
    The new network appears in the list on the Configuration page.
17. On the left navigation page, under **Inventory Management**, click **Collect Inventory**.

18. Under **Select Network Subnet(s)**, click the check box(es) for the network subnets on which you want to discover B5800 Branch Gateways.
19. Under **Select Device Types**, click the check box for **B5800 Branch Gateway**.
20. Do one of the following:
    - Click **Now** to run the inventory discovery job now.
    - Click **Schedule** to run the inventory discovery job at a scheduled date and time.

    When the job is completed, the B5800 Branch Gateway device(s) appear on the Collected Inventory page and on the Upgrade Management > Manage Software page.
21. Repeat steps 11 to 20 for each branch that is to be managed from System Manager.

Enabling SNMP and polling support

About this task

In order for the B5800 Branch Gateway control unit to be discovered and polled by an SNMP manager, its SNMP agent must be enabled and placed in the same read community as the SNMP manager.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **System Events** tab.
4. Select **SNMP Enabled**.
5. In the **SNMP Port** field, enter the UDP port number used by the SNMP agent to listen for and respond to SNMP traffic.

   The default is 161.
6. In the **Community (Read-only)** field, enter the community to which the device belongs for read access.

   This community name must match that used by the SNMP manager application when sending requests to the device. The community public is frequently used to establish communication and then changed (at both the SNMP agent and manager ends) for security.
7. Click **OK**.
8. Select **File > Save Configuration** to send the configuration back to the B5800 Branch Gateway and then select **reboot**.

After the reboot, the SNMP manager will be able to discover the control unit. The discovery includes the control unit type and the current level of core software.

Bulk importing of devices

Before you begin

Each B5800 Branch Gateway device has been added to an xml file. For information about the xml file containing the devices, see About the xml file containing the B5800 Branch Gateway devices on page 129.

About this task

Use this task to import the B5800 Branch Gateway devices from an xml file to System Manager.

Procedure

1. From the System Manager console, under **Elements**, select **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **More Actions > Import**.
4. On the Import Elements page, in the **Select File** field, enter the complete path of the xml file. Or, click **Browse** to locate the xml file.
5. Select one of the following error configuration options:
   - **Abort on first error**
   - **Continue processing other records**
6. Select one of the following import options:
   - To skip a matching record that already exists in the system during an import operation, click **Skip**.
   - To replace all data for an application, click **Replace**.
   - To merge application data so that you simultaneously perform an add and update operation of the application data, click **Merge**.
   - To delete the application data from the database that match the records in the xml file, click **Delete**.
7. Select one of the following schedule job options:
   - Click **Run immediately** to run the job now.
   - Click **Schedule later** and then select the date and time to run the job at a scheduled date and time.

8. Click **Import**.

About the xml file containing the B5800 Branch Gateway devices

To use the bulk import method to add the B5800 Branch Gateways to System Manager, you must first manually add each B5800 Branch Gateway device to an xml file.

The following sample shows the contents of an xml file for one B5800 Branch Gateway device.

```
<?xml version=”1.0” ?>
<RTSElements xmlns="http://www.avaya.com/rts"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<ApplicationSystems>
<ApplicationSystem name="B5800_2" isTrusted="false">
<Host ipaddress="192.168.42.2"></Host>
<ApplicationSystemType name="B5800 Branch Gateway"
version="0"></ApplicationSystemType>
      <Attributes>
                <Attribute name="Is B5800 for Linux"
value="false"></Attribute>
                <Attribute name="Service Login"
value="SMGRB5800Admin"></Attribute>
                <Attribute name="Service Password"
value="SMGRB5800Admin"></Attribute>
                <Attribute name="Device version"
value="6.2"></Attribute></Attributes>
</ApplicationSystem>
</ApplicationSystems>
</RTSElements>
```

The fields for each B5800 Branch Gateway device that you add to the xml file will be the same except for the following two fields which contain unique information for each device:

- **<ApplicationSystem name=”***B5800 device***”isTrusted=”false”>** where *B5800 device* is a unique name for this system.
- **<Host ipaddress=”***IP address***”></Host>** where *IP address* is a unique IP address for this system.

Adding the B5800 Branch Gateways to System Manager

About this task

Use this procedure to manually add the B5800 Branch Gateways to System Manager. This procedure must be performed for each B5800 Branch Gateway.

Procedure

1. From the System Manager console, under **Elements**, select **Inventory**.
2. On the Inventory page, click **Manage Elements**.

3. On the Elements page, click **New**.
4. On the New Elements page, in the **Type** drop-down box, select **B5800 Branch Gateway**.
5. On the New B5800 Branch Gateway page, in the **Name** field, enter a name for this B5800 Branch Gateway.
6. In the **Type** drop-down box, select **B5800 Branch Gateway**.
7. In the **Description** field, enter a description to help identify this B5800 Branch Gateway.
8. In the **Node** field, enter the IP address of the B5800 Branch Gateway.
9. Click the **Attributes** tab.
10. For the **SNMP Attributes Version**, click **V1**.
11. In the **Read Community** field, enter the community to which the device belongs for read access.
12. In the **Write Community** field, enter the community to which the device belongs for write access.
13. In the **Service Password** field, enter the service password. The default service password is the same as the Service Login (SMGRB5800Admin).
14. In the **Confirm Service Password** field, enter the service password again.
15. Click **Commit**.
16. Repeat steps 3 to 15 for each branch that is to be managed from System Manager.

Enabling WebLM licensing for the branch

About this task

If you are going to use WebLM licensing, you must enable the WebLM licensing feature for the branch. See Licensing on page 16 for more information.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **PLDS license**.
3. Click the check box for **Enable WebLM** to select this option.

4. In the **Domain Name (URL)** field, enter the IP address or fully qualified domain name of the System Manager WebLM server or other WebLM server that is being used.
5. In the **URN** field, enter the name of the WebLM server. The default is **WebLM/LicenseServer**.
6. In the **Port Number** field, use the up and down arrows to select the port number of the WebLM server. The default is **52233**.
7. Click **File > Save Configuration**.

Creating a system template

About this task

System templates are designed for new systems. They are not designed to distribute edited system configurations to the branches. Distributing an edited system template to a branch would override any local configuration changes that were made to a specific branch.

Note:

An edited system template could be pushed to multiple branches if it is certain that the branches are identical, the modified system configuration applies to all the branches, and there are no local configuration changes that will be overwritten.

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, in the left navigation pane, click **B5800 System Configuration**.
3. On the **B5800 Branch Gateway System Configuration Templates** page, do the following:
   a. Under **Supported B5800 Branch Gateway Types**, click the check box for **B5800**.
   b. Under **Templates List**, click **New**.
4. In the **Name** field, enter a name for this template.
5. In the **System Type** drop-down box, select **B5800**.
6. In the **Version** drop-down box, select the appropriate release.
7. To add more details to this system template, click **Details**.
   IP Office Manager is launched.
8. Complete the fields as appropriate.

9. When finished, select **File > Save Template and Exit**.

Uploading an auto attendant audio file

About this task

You are able to upload and convert audio files to System Manager that can be used in the B5800 Branch Gateway system configuration auto attendant feature. Once uploaded, from IP Office Manager you are able to select the audio files from the Auto Attendant page.

Note:

If you are using a system template, you can add the audio file to the template to push the audio file down to multiple B5800 Branch Gateway systems.

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the Templates page, click **B5800 System Configuration**.
3. On the B5800 Branch Gateway System Configuration Templates page, under Templates List, select **More Options > Manage Audio**.
4. On the Manage Audio page, click the **Browse** button to locate the .wav file you want to upload.
5. Click the **Upload** button.
   The voice file is uploaded to System Manager in the .c11 format that is required for Embedded Voicemail on B5800 systems. The file is automatically converted from the .wav format to the .c11 format.
6. When finished, click the **Done** button.

Applying the system template

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, in the left navigation pane, click **B5800 System Configuration**.

3. Under **Supported B5800 Branch Gateway Types**, click the check box for **B5800**.
4. Click **Show List**.
   All templates appear in the **Templates List**.
5. Select the template you want to apply, and then click **Apply**.
6. From the B5800 Branch Gateway Devices list, select the B5800 Branch Gateway(s) to which you want to apply the template.
7. Do one of the following:
   - Click **Now** to run the job now.
   - Click **Schedule** to run the job at a scheduled date and time.

Creating an endpoint template

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the **Templates** page, in the left navigation pane, click **B5800 Endpoint**.
3. On the **B5800 Branch Gateway Endpoint Templates** page, do the following:
   a. Under **Supported B5800 Branch Gateway Types**, click the check box for **B5800**.
   b. Under **Templates List**, click **New**.
4. In the **Name** field, enter a name for this endpoint.
5. In the **System Type** drop-down box, select **B5800**.
6. In the **Set Type** drop-down box, select the appropriate set type.
7. In the **Version** drop-down box, select **6.2**.
8. To configure more details for this endpoint, click the **Details** button.
   The IP Office Manager applet is launched.
9. On the Warning – Security page, click the check box to **Always trust content from this publisher**, and then click the **Yes** button.

   Note:

   After you select this check box for the first time, this warning page will no longer appear when you launch IP Office Manager.
10. On the Request Authentication page, click the **OK** button.

Note:

You do not need to provide a certificate on this page. This page will always appear when you launch IP Office Manager.

11. Complete the appropriate fields. The only fields you can edit in the user template are:
    - Locale
    - Priority
    - System Phone Rights
    - Profile

    All other fields in the user template are non-editable because they are not applicable to multiple users.
12. When finished, select **File > Save Template and Exit**.
    The template is saved in System Manager and listed in the Template List table.

Disabling unused trunks

About this task

Each B5800 Branch Gateway trunk card provides a fixed number of trunk ports with digital trunk ports supporting a fixed number of digital channels. By default the B5800 Branch Gateway configuration will have settings for all the possible trunks and channels.

In cases where the number of trunks or trunk channels in use is lower than the number supported by the trunk card, the unused trunks and channel must be disabled.

Important:

Failure to do this will cause problems with outgoing calls.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **Line**.
3. For each line, set those lines or channels that are not connected or not being used as **Out of Service**.

   The location of the relevant setting varies for each trunk type.

4. For **Analog Trunks**, set the **Trunk Type** to **Out of Service**.
5. For **BRI, E1 PRI, S0 and QSIG Trunks**, set the channels quantities to match the actual subscribed channels.
6. For **T1, T1 PRI and E1R2 Trunks**, select the Channels tab. Then do the following:

   Select those channels that are not used and click **Edit**.

   - For T1 set the **Type** to **Out of Service**
   - For T1 PRI set the **Admin** field to **Out of Service**.
   - For E1R2 trunks set the **Line Signalling Type** to **Out of Service**.
7. Select **File > Save Configuration**.

Digital trunk clock source

About this task

Digital trunks require the telephone system at each end of the trunk to share a clock signal to ensure synchronization of call signalling. The B5800 Branch Gateway can obtain and use the clock signal from any of its digital trunks. Typically the clock signal provided by a digital trunk from the central office exchange is used as this will be the most accurate and reliable clock source.

To do this, the **Clock Quality** setting on each line in the B5800 Branch Gateway configuration is set to one of the following:

- **Network**

  If available, the clock signal from this trunk should be used as the B5800 Branch Gateway clock source for call synchronization. If several trunk sources are set as Network, the B5800 Branch Gateway will default to using one as detailed below.

- **Fallback**

  If available, the clock signal from this trunk can be used as the clock source if none of the trunks set as Network are providing a clock source.

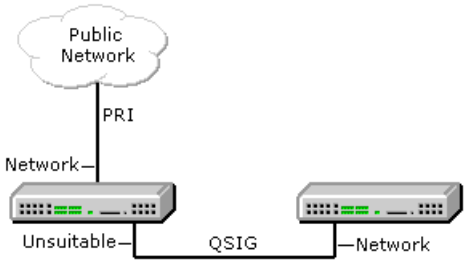
- **Unsuitable**

  The clock source from this trunk will never be used as the B5800 Branch Gateway clock source.

If no clock source is available the B5800 Branch Gateway can use its own internal clock if necessary.

In the example below the first B5800 Branch Gateway is set to use the public network trunk as its clock source and ignoring the possible clock source from the QSIG trunk. The other B5800 Branch Gateway system is using the clock signal received from the first B5800 Branch

Gateway on its QSIG trunk as its clock source. Thus both systems are using the same clock source and that clock source is the public network exchange.



When multiple trunks with the same setting are providing clock signals, trunks are used in the order of slots 1 to 4 and then by port on each slot.

The current clock source being used by an B5800 Branch Gateway system is shown on the Resources page within the IP Office System Status Application.

Setting a trunk clock quality setting

About this task

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **Line**.
3. For each digital line, do the following:
   a. Select the line.
   b. On the **Line** tab, select whether that trunk should provide the clock source for the network or whether the trunk is unsuitable.

      Note:

      For E1R2 trunks the **Clock Quality** setting is on the **Advanced** tab
4. Ensure that only one trunk is set to **Network**. This should preferably be a direct digital trunk to the central office exchange.
5. Set one other trunk to **Fallback** in case the selected network trunk connection is lost.

   Note:

   If possible this should be a trunk from a different provider since that reduces the chances of both sources failing at the same time.
6. Ensure that all other digital trunks are set as **Unsuitable**.

7. Select **File > Save Configuration**.

Setting the trunk prefixes

About this task

Where a prefix has been implemented for outgoing calls, that same prefix needs to be added to trunk settings. The prefix is then used as follows:

- On incoming calls the prefix is added to any incoming ICLID received with the call. That allows the ICLID to be used by B5800 Branch Gateway phones and applications to make return calls.
- On outgoing calls, the short codes used to route the call to a trunk must remove the dialing prefix.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **Line**.
3. For each line enter the prefix. The location of the relevant setting varies for each trunk type.
    - For analog trunks, select the **Line Settings** tab and enter the prefix in the **Prefix** field.
    - For T1 and T1 PRI trunks, select the **PRI 24 Line** tab and enter the prefix in the **Prefix** field.
    - For BRI, E1 PRI, and QSIG trunks, select the **PRI Line** tab and enter the appropriate prefix in the following fields:
        - Prefix
        - National Prefix
        - International Prefix
4. Select **File > Save Configuration**.

SIP trunk prefixes

The prefix fields Prefix, National Prefix, Country Code and International Prefix are available with the SIP line settings. These fields are used in the following order:

1. If an incoming number (called or calling) starts with the + symbol, the + is replaced with the International Prefix.
2. If the Country Code has been set and an incoming number begins with that Country Code or with the International Prefix and Country Code, they are replaced with the National Prefix.
3. If the Country Code has been set and the incoming number does not start with the National Prefix or International Prefix, the International Prefix is added.
4. If the incoming number does not begin with either the National Prefix or International Prefix, then the Prefix is added.

For example, if the SIP line is configured with the following prefixes, the numbers are processed as described in the table below.

- Line Prefix: 9
- National Prefix: 90
- International Prefix: 900
- Country Code: 44

Number Received	Processing	Resulting Number
+441707362200	Following rule 1 above, the + is replaced with the International Prefix (900), resulting in 900441707362200. The number now matches the International Prefix (900) and Country Code (44). Following rule 2 above they are replaced with the National Prefix (90).	901707362200
00441707362200	Following rule 2 above the International Prefix (900) and the Country Code (44) are replaced with the National Prefix (90).	90107362200
441707362200	Following rule 2 above, the Country Code (44) is	901707362200

Number Received	Processing	Resulting Number
	replaced with the National Prefix (90).	
6494770557	Following rule 3 above the International Prefix (900) is added.	9006494770557

Administering a Session Manager line for each branch

This section provides the procedures required to configure a Session Manager line between each branch site and the headquarters site.

This section also describes how the B5800 Branch Gateway uses a configured Session Manager line to handle incoming and outgoing calls to and from the branch and explains how a second Session Manager line can be configured for Session Manager line redundancy.

- See Enabling SIP trunk support on page 139. Use this procedure to configure the IP Office LAN interface which will be used for the Session Manager line connection to the Avaya Aura® Session Manager.
- See Setting the branch prefix and local number length for extension numbering on page 140. Use this procedure to set the prefix number for the B5800 Branch Gateway and the required extension length.
- See Changing the default codec selection on page 143. Use this procedure to set the preferred order for codec negotiation. This can be done as a system default and also for each individual SIP and Avaya Aura® Session Manager line.
- See Adding an Avaya Aura Session Manager line on page 145. Use this procedure to create a Session Manager line for calls to the Avaya Aura® Session Manager.
- See Setting up outgoing call routing on page 151. Use this procedure to create short codes for routing calls to the Avaya Aura® Session Manager line when the required destination or resource is on another branch of the Avaya Aura® network.
- See How the B5800 Branch Gateway uses a configured Session Manager line on page 153.
- See Avaya Aura Session Manager line redundancy on page 150.

Enabling SIP trunk support

About this task

Before adding any SIP trunks, including Avaya Aura® Session Manager lines, the B5800 Branch Gateway system must be configured for SIP trunk operation. The system has 2 LAN

interfaces, LAN1 and LAN2 (the physical ports are labeled LAN and WAN respectively). Either can be used for the Avaya Aura® Session Manager line operation.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **System**.
3. Click the **LAN1** or **LAN2** tab as appropriate depending on which branch site LAN interface will be used for the data connection to the Avaya Aura® network.
4. Confirm that the IP address and IP Mask fields are set correctly for the site.
5. Click the **VoIP** tab.
6. Select the **SIP Trunks Enable** option. This is required for Avaya Aura® Session Manager trunk support.

   Note:

   The **SIP Registrar Enable** setting and settings in the **SIP Registrar** tab relate to SIP extension support and therefore do not affect Avaya Aura® Session Manager lines. The settings in the **Network Topology** tab relate to external SIP trunks. Those settings are not used by Avaya Aura® Session Manager lines, which use open internet across the customer WAN.
7. Click **OK**.
8. Select **File > Save Configuration**.
   The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Setting the branch prefix and local number length for extension numbering

About this task

Each B5800 Branch Gateway system in the network should have a unique branch number. That number is added as a prefix to the caller's extension number for calls routed from native extensions to the Avaya Aura® Session Manager. This means that native extensions are defined on the B5800 Branch Gateway without the branch prefix, so that when the branch

prefix is added, the number is the correct length and format expected by Avaya Aura®Session Manager.

The prefix is also used in the Avaya Aura® Session Manager configuration to create unique dial patterns for routing calls to the appropriate B5800 Branch Gateway.

Beginning in B5800 Branch Gateway R6.2, you have the option to leave the Branch Prefix field blank. If you do not configure the Branch Prefix, the native extensions must be defined with the full enterprise number. You are also able to leave the Local Number Length field blank.

By default B5800 Branch Gateway systems use 3-digit extension numbering starting from 200. The existing allocated numbers can be changed in bulk using the **Tools > Extension Renumber** option. This will add or remove a set value from all existing extension numbers in the configuration.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **System**.
3. Click the **System** tab.
4. Set the following fields as appropriate:
   - Branch Prefix (optional)
   - Local Number Length (optional)
   - Proactive
   - Reactive

   These 4 fields are the key settings for B5800 Branch Gateway operation. See System tab field descriptions on page 141 for more information.
5. Click **OK**.
6. Select **File > Save Configuration**.
   The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

System tab field descriptions

Name	Range or Default	Description
Branch Prefix	Range = 0 to 999999999	This number is used to identify the B5800 Branch Gateway system within the

Name	Range or Default	Description
		Avaya Aura® network. The branch prefix of each B5800 Branch Gateway system must be unique and must not overlap. For example 85, 861 and 862 are okay, but 86 and 861 overlap. On calls routed via an Avaya Aura®Session Manager line, the branch prefix is added to the caller's extension number. Beginning in B5800 Branch Gateway R6.2, you have the option to leave the Branch Prefix field blank. If you do not configure the Branch Prefix, the native extensions must be defined with the full enterprise number.
Local Number Length	Range = Blank (Off) or 3 to 9 for native extensions	This field sets the default length for extension numbers for extensions, users, and hunt groups added to the B5800 Branch Gateway configuration. Entry of an extension number of a different length will cause an error warning by Manager. The combined **Branch Prefix** and **Local Number Length** should not exceed 15 digits. Beginning in B5800 Branch Gateway R6.2, you have the option to leave the Local Number Length field blank.
Proactive	Default = 60 seconds, Range = 60 to 100000 seconds	The B5800 Branch Gateway sends regular SIP OPTION messages to the Avaya Aura®Session Manager line in order to check the status of the line. This setting controls the frequency of the messages when the Avaya Aura®Session Manager line is currently in service.

Name	Range or Default	Description
Reactive	Default = 60 seconds, Range = 10 to 3600 seconds	The B5800 Branch Gateway sends regular SIP OPTION messages to the Avaya Aura®Session Manager line in order to check the status of line. This setting controls the frequency of the messages when the Avaya Aura®Session Manager line is currently out of service.

Changing the default codec selection

About this task

By default, all B5800 Branch Gateway IP trunks and extensions use automatic codec negotiation. The default negotiation order is G729(a) 8K CS-ACELP, G711 U-Law 64K, G711 A-Law 64K, and G723.1 6K3 MP-MLQ. G.722 64K is also available.

If bandwidth between the B5800 Branch Gateway and Avaya Aura® sites is sufficient, change the first default preference to one of the G711 codecs. Note that the specific setting for individual branch trunks and extensions can be set to override the system setting if necessary.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **System**.
3. Click the **Codecs** tab.
4. In the **Available Codecs** section, check the appropriate codecs and move them to the **Selected** section.
   The order of the codecs listed in the **Selected** section indicates the preferred codec order for trunks and extensions that are using automatic codec negotiation. See Automatic codec preference settings on page 144 for more information.
5. Click **OK**.
6. Select **File > Save Configuration**.

The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Automatic codec preference settings

Setting	Selected Preference	2nd Preference	3rd Preference	4th Preference
G.729	G729(a) 8K CS-ACELP	G711 U-Law 64K	G711 A-Law 64K	G723.1 6K3 MP-MLQ
G.723	G723.1 6K3 MP-MLQ	G729(a) 8K CS-ACELP	G711 U-Law 64K	G711 A-Law 64K
G.711 U-Law	G711 U-Law 64K	G711 A-Law 64K	G729(a) 8K CS-ACELP	G723.1 6K3 MP-MLQ
G.711 A-Law	G711 A-Law 64K	G711 U-Law 64K	G729(a) 8K CS-ACELP	G723.1 6K3 MP-MLQ

G.722 64K codec is also supported on systems with IP500 VCM or IP500 Combo cards. By default, the G.722 64K codec is not used.

Changing the maximum SIP sessions

About this task

The Maximum SIP Sessions setting determines the number of concurrent sessions allowed across all SIP trunks (SM line and public SIP trunks). Setting Maximum SIP Sessions to a specific value requires a corresponding quantity of B5800 Branch Gateway SIP Trunk Session licenses. If B5800 Branch Gateway cannot obtain the required license quantity then the configuration change will be rejected. If the required license quantity cannot be obtained or renewed for an already-configured value of Maximum SIP Sessions, then the B5800 Branch Gateway will be in License Error mode, or in License Restricted mode if the 30-day grace period has expired. The license error can be resolved either by making a sufficient quantity of SIP Trunk Session licenses available, or by reducing the configured Maximum SIP Sessions setting to a value for which sufficient license quantity is available. Regardless of the license mode, the number of concurrent SIP sessions allowed in system operation is determined by the Maximum SIP Sessions setting.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.

2. In the left navigation pane, click **System**.
3. Click the **Telephony** tab.
4. Click the **Telephony** sub-tab.
5. In the **Maximum SIP Sessions** box, click the up or down arrows to select the number that matches the Maximum SIP Trunk Sessions licensed for the system.

   To see the Maximum SIP Trunk Sessions licensed for the system, in the left navigation pane, select **PLDS License**.
6. Click **OK**.
7. Select **File > Save Configuration**.

Adding an Avaya Aura® Session Manager line

About this task

Use this procedure to add an Avaya Aura®Session Manager line to the B5800 Branch Gateway system configuration. If multiple Avaya Aura®Session Managers are available at the headquarters site, an additional Avaya Aura® Session Manager line can be added for Session Manager line redundancy. The two Session Manager lines are prioritized based on the line number. The lower line number is considered the primary Session Manager line. Based on the priority of the Session Manager lines designated by the line number, the active line to which the B5800 Branch Gateway sends all calls will always be the highest priority Session Manager line in service. See the IP Office Manager online help and Avaya Aura Session Manager line redundancy on page 150 for more information.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **Line**.
3. Click the **New** icon and select **SM Line**.
4. Configure the line settings as appropriate. See Session Manager tab field descriptions on page 146 for more information.
5. Click **OK**.
6. Click the **VoIP** tab.

7. Click the **Re-Invite Supported** check box to select this option.
8. Click the **Allow Direct Media Path** check box to select this option. You can select this option only if you selected **Re-Invite Supported**.
9. Configure the remaining fields as appropriate. See VoIP tab field descriptions on page 147 for more information.
10. Click **OK**.
11. Select **File > Save Configuration**.
    The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Session Manager tab field descriptions

Name	Description
Line Number	This value is automatically assigned by B5800 Branch Gateway and should be unique for each line added to the configuration.
In Service	The default setting is enabled. This option can be used to manually take the Session Manager line out of service. It does not reflect or set the actual state of the line.
SM Domain Name	This name should match a SIP domain defined in the Session Manager system's SIP Domains table. Unless there are reasons to do otherwise, all the B5800 Branch Gateway systems in the Avaya Aura® network can share the same domain. **Note:** See Viewing the SIP domains on page 166 for a list of SIP domains defined in Session Manager.
SM Address	Enter the IP address of the Session Manager that the line should use in the Avaya Aura® network. The same Session Manager should be used for the matching Entity Link entry in the Avaya Aura® configuration.
Outgoing Group ID	The default setting is 99999. This value is not changeable. However note the value as it is used in B5800 Branch Gateway short codes used to route calls to the Session Manager.

Name	Description
Prefix	This field is blank by default. This prefix will be added to any source number received with incoming calls.
Max Calls	The default setting is 10. This value sets the number of simultaneous calls allowed between B5800 Branch Gateway and Session Manager using this connection. Each call uses one of the available licenses that are shared by all SIP trunks configured in the system.
URI Type	When SIP or SIPS is selected in the drop-down box, the SIP URI format is used (for example, name@example.com). This affects the From field of outgoing calls. The To field for outgoing calls will always use the format specified by the short codes used for outgoing call routing. Recommendation: When SIP Secured URI is required, the URI Type should be set to SIPS. SIPS can be used only when Layer 4 Protocol is set to TLS.
Layer 4 Protocol	This can be set to TLS or TCP. Set to TLS to choose SIPS as the URI Type when SIP Secured URI is required.
Send Port	When Layer 4 Protocol is set to TLS, the default setting is 5061. When Layer 4 Protocol is set to TCP, the default setting is 5060.
Listen Port	When Layer 4 Protocol is set to TLS, the default setting is 5061. When Layer 4 Protocol is set to TCP, the default setting is 5060.

VoIP tab field descriptions

Name	Range or Default	Description
Codec Selection	Default = System Default	This field defines the codec or codecs offered during call setup. When System Default is selected, the codec list shown matches the codecs set in the system-wide

Name	Range or Default	Description
		Default Codec Selection (System > Codecs).
Fax Transport Support	Default = None	This option is only selectable if the option **Re-Invite Supported** is also selected. If enabled, the B5800 Branch Gateway is able to support the sending and receiving of faxes via the Avaya Aura® Session Manager line using the T38 protocol. The settings for T38 are set on the T38 Fax tab.
Call Initiation Timeout	Default = 4 seconds	The B5800 Branch Gateway sends regular OPTION messages to each Avaya Aura®Session Manager line in order to check the lines in or out of service status. If a response is not received within this timeout, the line is treated as being out of service.
DTMF Support	Default = RFC2833	This setting is used to select the method by which DTMF key presses are signaled to the remote end. The supported options are **In Band**, **RFC2833** or **Info**.
Media Security	Default = Disable	Media security is not required. All media sessions (audio, video, and data) will be enforced to use RTP only.
Advanced		This option provides additional media security options. These options are not supported in B5800 Branch Gateway R6.2.
VoIP Silence Suppression	Default = Off	When selected, this option will detect periods of silence on any call over the line and will not send any data during those silent periods.

Name	Range or Default	Description
Allow Direct Media Path	Default = On	This setting controls whether connected calls must remain routed via the B5800 Branch Gateway or can be routed alternately if possible within the network structure. • If enabled, connected calls can take routes other than through the B5800 Branch Gateway. This removes the need for a voice compression channel. • If disabled or not supported at one end of the call, the call is routed via the B5800 Branch Gateway. However RTP relay support allows calls between devices using the same audio codec to not require a voice compression channel.
Re-Invite Supported	Default = On	When enabled, Re-Invite can be used during a session to change the characteristics of the session, for example when the target of an incoming call or a transfer does not support the codec originally negotiated on the trunk.
Use Offerer's Preferred Codec	Default = Off	Normally for SIP calls, the codec preference of the answering end is used. This option can be used to override that behavior and use the codec preferences offered by the caller.
Codec Lockdown	Default = Off	Supports RFC 3264 Section 10.2 when Re-Invite Supported and Codec Lockdown are enabled. In response to a SIP offer with a list of codecs supported, some SIP user agents supply a SDP answer that also lists multiple codecs. This means

Name	Range or Default	Description
		that the user agent may switch to any of those codecs during the session without further negotiation. The system does not support multiple concurrent codecs for a session, so loss of speech path will occur if the codec is changed during the session. If codec lockdown is enabled, when the system receives an SDP answer with more than one codec from the list of offered codecs, it sends an extra re-INVITE using just a single codec from the list and resubmits a new SDP offer with just the single chosen codec.

Avaya Aura® Session Manager line redundancy

In an Avaya Aura® network that includes multiple Avaya Aura® Session Managers for redundancy, the B5800 Branch Gateway system can be configured with a secondary Avaya Aura® Session Manager line. If for any reason the B5800 Branch Gateway system's primary Avaya Aura® Session Manager line goes out of service, the system will automatically attempt to use the secondary Avaya Aura® Session Manager line. Prioritization of the Session Manager lines is determined by the line number configured for a particular Session Manager line. For example, if the first Session Manager line is configured with line number 17 and the second Session Manager line is configured with line number 18, then line number 17 has the higher priority and is considered the primary Session Manager line. If for some reason you want to designate the secondary Session Manager line as the primary line, you must change one or both of the line numbers associated with the Session Manager lines so that the secondary Session Manager line number is lower than that of the primary line.

The redundancy operation of the Session Manager lines is based on line prioritization. The active line to which B5800 Branch Gateway sends all calls is always the highest priority Session Manager line in service. If the primary Session Manager line is in service, it is the active line for sending calls. If the connection to the primary Session Manager line is lost, causing B5800 Branch Gateway to switch to the secondary Session Manager line, when the primary line comes back up, B5800 Branch Gateway will switch back to the primary B5800 Branch Gateway line.

If all available channels of the current Avaya Aura®Session Manager line are in use, the B5800 Branch Gateway will not overflow calls to the other Avaya Aura®Session Manager line.

However, if PSTN trunk fallback has been configured, the other Avaya Aura®Session Manager line will be used. See PSTN trunk fallback on page 294 for more information.

Avaya Aura®Session Manager line service status checks

The B5800 Branch Gateway system sends regular SIP OPTIONS messages to any Avaya Aura® Session Manager lines in its configuration. The Proactive and Reactive settings on the B5800 Branch Gateway system's System tab set how often the SIP OPTIONS messages are sent in seconds. The Proactive setting is used for an Avaya Aura® Session Manager line currently thought to be in service. The Reactive setting is used for an Avaya Aura® Session Manager line currently thought to be out of service.

- If a response is received and is not a 408, 500, 503 or 504 response, the Avaya Aura® Session Manager line is treated as in service; otherwise the line is treated as being out of service.
- If no response is received within 32 seconds (SIP Timer F), the line is treated as being out of service.
- If the line is out of service, and call comes from the trunk, the trunks status is changed back to in service.
- If the line is in service, a call may fail due to either being unable to deliver the message or receive a 100 response within a configured timeout. The line will not go out of service because this may be a temporary failure due to a busy system.

Secondary Avaya Aura® Session Manager line configuration

The secondary Avaya Aura® Session Manager line is configured in the same way as the primary Avaya Aura®Session Manager line. The only difference required is to set the **SM Address** field to the address of the alternate Avaya Aura®Session Manager from the one being used by the primary Avaya Aura® Session Manager line.

Setting up outgoing call routing

About this task

For calls from extensions on the B5800 Branch Gateway system to other numbers within the network, system short codes are used to route the calls to the Avaya Aura® Session Manager line. The Avaya Aura® Session Manager then performs the routing to determine where the call should go.

Note:

See Branch PSTN call routing examples on page 289 for information on routing back to the branch for fallback alternate routes.

Note:

If using Avaya Aura® Conferencing 7.0, the B5800 Branch Gateway short code should include routing to Session Manager any call that is made to the Avaya Aura® Conferencing 7.0 number.

Ideally the number of such system short codes should be kept to a minimum and the same short codes used on all branches in order to ease maintenance. This is where using a uniform

dial plan for all branches helps, as explained in Dial plan considerations on page 36. For our example, the uniform dial plan allows the same single short code to be used at all branches.

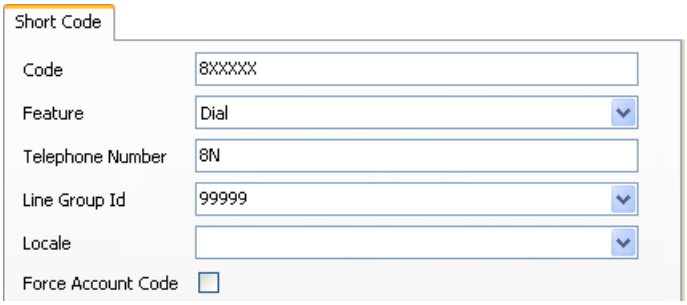
See the Manager context-based help for more information on creating short codes.

Note:

In the Distributed branch user model, when a short code match occurs and the telephone number to be sent to the Avaya Aura® Session Manager line begins with the B5800 Branch Gateway system's own branch prefix, the prefix is removed and the call is re-targeted locally on the B5800 Branch Gateway system.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **Short Code**.
3. Click the **New** icon and select **Short Code**.



4. Configure the settings as appropriate. See Short Code tab field descriptions on page 153 for more information.

   Note:

   To view more information about the system short codes, press F1. In particular, see the description of the **Dial** short code.

5. Click **OK**.
6. Select **File > Save Configuration**.

Short Code tab field descriptions

Name	Description
Code	Enter the number dialed by users that should be matched to this short code. Use **X** wildcards for any single digit.
Feature	Leave this field set as **Dial**.
Telephone Number	Set this field to match a number that should be passed to the Avaya Aura® Session Manager for routing against its dialing pattern matches. The **N** wildcard can be used to match any wildcards in the **Code**. **Note:** Add SS to the entry in this field to have the caller ID passed to the Session Manager line. For example, if you are entering 8N in the Telephone Number field, enter 8NSS.
Line Group Id	Set the **Line Group ID** to match the **Outgoing Group** settings used in the SM lines URI setting.
Local	Features that transfer the caller to Voicemail Pro can indicate the language locale required for prompts. This is subject to the language being supported and installed on the voicemail server. The default is blank.
Force Account Code	When selected, for short codes that result in the dialing of a number, the user is prompted to enter a valid account code before the call is allowed to continue. The default is **Off**.

How the B5800 Branch Gateway uses a configured Session Manager line

Once configured and in operation, the Avaya Aura® Session Manager line is used as follows.

Outgoing calls from a branch

In the Distributed branch user model, if the outgoing call begins with the branch's own prefix, the prefix is removed and the call is targeted locally to the matching native user or hunt group

extension number. If there is no matching extension number, the call is targeted to any matching system short code.

Incoming calls to a branch

Incoming calls on an Avaya Aura®Session Manager line are treated as being internal calls and do not go through the B5800 Branch Gateway system's Incoming Call Route settings.

- If the destination of the incoming call on the Avaya Aura® Session Manager line starts with the system's branch prefix, the prefix is removed. The call is then targeted to the matching native user or hunt group extension number. If there is no matching extension number, the call is targeted to any matching system short code.
- If the destination of the incoming call on the Avaya Aura® Session Manager line does not start with the system's branch prefix, the whole number is checked for a match against system short codes.

Line status detection

The B5800 Branch Gateway system sends regular OPTION messages to any Avaya Aura® Session Manager lines in its configuration. The Proactive and Reactive settings on the B5800 Branch Gateway system's **System** tab set how often the OPTION messages are sent in seconds. The Proactive setting is used for an Avaya Aura® Session Manager line currently thought to be in service. The Reactive setting is used for an Avaya Aura® Session Manager line currently thought to be out of service.

- If a response is received and is not a 408, 500, 503 or 504 response, the Avaya Aura® Session Manager line is treated as in service; otherwise the line is treated as being out of service.
- If the line is out of service, and call comes from the trunk, the trunks status is changed back to in service.
- If the line is in service, a call may fail due to either being unable to deliver the message or receive a 100 response within a configured timeout. The line will not go out of service because this may be a temporary failure due to a busy system.
- In addition each Avaya Aura® Session Manager line can be manually set to in or out of service using the In Service option on the Avaya Aura® Session Manager line's **Session Manager** tab.

Enabling branch SIP extension support

About this task

Before adding any SIP extensions, the B5800 Branch Gateway system must be enabled for SIP extension support. Use this procedure to configure the B5800 Branch Gateway to support the addition of SIP extensions.

Important:

The configuration changes in the following procedure will require the B5800 Branch Gateway system to be rebooted.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **System**.
3. Click the **LAN1** or **LAN2** tab, depending on which branch site LAN interface will be used for the SIP extensions.
4. In the **LAN Settings** tab, make a note of the IP Address and IP Mask details as these will be required during the SIP extension configuration.
5. Click the **VoIP** tab.
6. Check the **SIP Registrar Enable** check box. This is necessary for support of SIP extensions directly by the branch or when providing survivability support for Avaya Aura® SIP extensions.
7. Click **OK**.
8. Click the **SIP Registrar** tab.
9. Configure the fields on this tab as appropriate. See SIP Registrar tab field descriptions on page 155 for more information.
10. Click **OK**.
11. Select **File > Save Configuration**.
    The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

SIP Registrar tab field descriptions

Name	Default	Description
Domain Name	Default = Blank	This is the local SIP registrar domain name that will be needed by SIP devices in order to register with the B5800 Branch Gateway. If this field is left blank, registration is against the LAN IP address. For our examples we have been using a domain, **example.com**.

Name	Default	Description
Layer 4 Protocol	Default = UDP, TCP, TLS • UDP, SIP port = 5060 • TCP, SIP port = 5060 • TLS, SIP port = 5061	This is the transport protocol for SIP traffic between the B5800 Branch Gateway and SIP extension devices.
Challenge Expiry Time (sec)	Default = 10	The challenge expiry time is used during SIP extension registration. When a device registers, the SIP Registrar will send a challenge back to the device and waits for an appropriate response. If the response is not received within this timeout the registration is failed.

Chapter 9: Managing B5800 Branch Gateways from System Manager

This chapter provides tasks that you will use as you configure B5800 Branch Gateways that are managed from System Manager.

Editing a B5800 Branch Gateway system configuration from System Manager

Before you begin

Avaya Aura® System Manager has been set up to launch IP Office Manager. See Setting up System Manager to launch IP Office Manager on page 112.

About this task

Use this procedure to launch IP Office Manager from System Manager to edit a B5800 Branch Gateway system configuration.

Note:

You cannot configure users when editing a B5800 Branch Gateway system configuration from System Manager. User configuration is performed from System Manager User Management. For more information, see Restrictions when editing a B5800 Branch Gateway system configuration from System Manager on page 158.

Procedure

1. From the System Manager console, under **Elements**, select **B5800 Branch Gateway**.
2. In the left navigation pane, click **System Configuration**.
3. On the B5800 Branch Gateway System Configuration page, select the B5800 Branch Gateway device whose system configuration you want to edit.
4. Click **Edit**.
   The IP Office Manager application is launched.

   Note:

   If the B5800AdminLite.exe file has not been downloaded to the System Manager server, an error message appears that says **The system cannot find the file specified**. If you receive this message, click **OK**. Then see Setting up System

Manager to launch IP Office Manager on page 112 for the procedure to install the B5800AdminLite.exe file on the System Manager server.

Note:

If this is the first time you are attempting to edit a B5800 Branch Gateway device through System Manager from this PC, and IP Office Manager has not yet been installed on this PC, the following message appears:

B5800 Branch Gateway Manager not installed.

Avaya B5800 Branch Gateway Manager is not installed on this machine. To complete the current task, you must download and install Avaya B5800 Branch Gateway Manager. After you complete this installation restart the machine. Refer to the Release Notes/Online help.

Do you want to download Avaya B5800 Branch Gateway Manager from the server now?

If you receive this message, click **Yes**. Then go to step 4 in Installing IP Office Manager from the System Manager server to a PC on page 114 for the procedure to install IP Office Manager on the PC.

Restrictions when editing a B5800 Branch Gateway system configuration from System Manager

When you edit the system configuration of a B5800 Branch Gateway device that is managed from System Manager, IP Office Manager is launched in system mode. The following restrictions apply when editing a B5800 Branch Gateway system configuration from System Manager with IP Office Manager in system mode.

- **Extension** is visible in the **Extn** tab only but is disabled.
- All users (other than **NoUser** and **RemoteManager**) are visible in the **User** tab only but are disabled.
- **NoUser** has **User** and **Source Number** tabs visable and editable. The rest of the tab is not visable and therefore not editable.
- **RemoteManager** has the **User** tab visable and editable. The rest of the tab is not visable and therefore not editable.

The User Management feature available in System Manager is used to manage users and extensions on B5800 Branch Gateway systems that are centrally managed from System Manager. See User administration on page 185 for more information.

Note:

Do not use IP Office Manager that is connected directly to the B5800 Branch Gateway device to edit users and extensions on systems that are centrally managed from System Manager.

Changes made to users and extensions in this way will not be synced back to System Manager.

For more information about the two management methods, that is, central management from System Manager or local management from IP Office Manager, see Management on page 14. Do not use both of these management methods to configure and manage users and extensions on a B5800 Branch Gateway system.

System Manager does not support the configuration of User Rights on B5800 Branch Gateway systems. Similar functionality of applying selected user settings to groups of users is available from the System Manager user template capability.

About disabling the System Manager administration feature for a B5800 Branch Gateway

If the B5800 Branch Gateway is centrally managed by System Manager and you want to administer the B5800 Branch Gateway using IP Office Manager that is directly connected to the branch, for example to install an individual PLDS license file, you must first disable the System Manager administration feature for the branch. Disabling the System Manager administration feature for a branch can be performed from System Manager or from IP Office Manager if the network connection to System Manager is not available.

After you disable the System Manager administration feature for a branch and administer the branch using IP Office Manager, you must synchronize the B5800 Branch Gateway with System Manager to synchronize the changes and return the System Manager administration feature for the branch to the enabled state. You can also manually enable the System Manager administration feature for a branch using either of the procedures listed below and clicking the check box for **Under SMGR Administration** to enable the feature.

To disable the System Manager administration feature for a branch, see one of the following:

- Disabling the System Manager administration feature for the branch from System Manager on page 160
- Disabling the System Manager administration feature for the branch from IP Office Manager on page 160

To synchronize the B5800 Branch Gateway with System Manager, see Synchronizing B5800 Branch Gateway with System Manager on page 162. Some configuration changes cannot be synced with System Manager. See Configuration changes performed through Manager that cannot be synced with System Manager on page 162 for more information.

Disabling the System Manager administration feature for the branch from System Manager

Procedure

1. From the System Manager console, under **Elements**, click **B5800 Branch Gateway**.
2. On the B5800 Branch Gateway Element Management page, in the left navigation pane, click **Security Configuration**.
3. On the B5800 Branch Gateway Security Configuration page, click the radio button for the appropriate branch.
4. Click **Edit**.
5. In the Security Settings pane, select **Services > Configuration**.
6. In the Service Details tab, click the check box for **Under SMGR Administration** to deselect this option.

   Note:

   This check box is checked by default and you are not able to administer the branch through Manager. To be able to use Manager to administer the branch, this check box must be unchecked.
7. Click **OK**.
8. Select **File > Save Configuration**.

Disabling the System Manager administration feature for the branch from IP Office Manager

Procedure

1. Start IP Office Manager.
2. Select **File > Advanced > Security Settings**.

   Note:

   If the **Security Settings** option does not appear under Advanced, do the following:

   a. Select **File > Preferences**.

b. In the IP Office Manager Preferences dialog box, click the **Set Simplified View as default** check box to deselect this option
c. Click **OK**.
d. Close and restart IP Office Manager.

3. In the **Select B5800** window, click the check box for the appropriate system.
4. Click **OK**.
5. In the Security Service User Login window, enter a user name and password of an account that has security configuration access to the B5800 Branch Gateway system.

   The defaults are **security** and **securitypwd**.
6. In the Security Settings pane, select **Services > Configuration**.
7. In the Service Details tab, click the check box for **Under SMGR Administration** to deselect this option.

   Note:

   This check box is checked by default and you are not able to administer the branch through IP Office Manager. To be able to use IP Office Manager to administer the branch, this check box must be unchecked.
8. Click **OK**.
9. Select **File > Save Security Settings**.

Enabling the Security Settings option for the branch

About this task

To disable the System Manager administration feature for a branch that is centrally managed by System Manager, you must have access to the Security Settings for that branch. If the branch configuration has not yet been opened from IP Office Manager, the **Security Settings** option is not available. To enable the **Security Settings** option, you must de-select the **Set Simplified View as default** option in the IP Office Manager Preferences window. Once that is done, the **Security Settings** option becomes available for that branch.

Note:

This task needs to be performed only one time.

Procedure

1. Start IP Office Manager.
2. Select **File > Preferences**.

3. In the **Preferences** tab, click the **Set Simplified View as default** check box to de-select this option.
4. Click **OK**.
5. Close IP Office Manager.
6. See Disabling the System Manager administration feature for the branch from System Manager on page 160.

Synchronizing B5800 Branch Gateway with System Manager

About this task

Some configuration changes cannot be synced with System Manager. See Restrictions when editing a B5800 Branch Gateway system configuration from System Manager on page 158 for more information.

Procedure

1. On the System Manager console, under **Elements**, click **Inventory**.
2. In the left navigation pane, click **Synchronization > B5800 Branch Gateway**.
3. Click the check box for the B5800 Branch Gateway system whose configuration you want to sync with System Manager.
4. Do one of the following:
   - Click **System Configuration** to sync only system configuration data with System Manager.
   - Click **User** to sync only user data with System Manager.
   - Click **System Configuration and Users** to sync system configuration and user data with System Manager.
5. Do one of the following:
   a. Click **Now** to run the synchronization job now.
   b. Click **Schedul**e to run the synchronization job at a scheduled date and time.

Configuration changes performed through Manager that cannot be synced with System Manager

You are able to disable System Manager administration for a B5800 Branch Gateway and configure the B5800 Branch Gateway device locally through IP Office Manager. To do this, you

must first disable System Administration for the branch and then enable System Administration for the branch after you make your configuration changes. Then you must synchronize those changes with System Manager.

There are some configuration changes that cannot be synchronized with System Manager. Those tasks should not be performed locally through IP Office Manager for branches that are centrally managed by System Manager. Configuration changes that cannot be synchronized and therefore should not be performed locally are:

- adding users or extensions
- editing user core attributes (that is, name, number, password, or extension number)
- changing any of the following security configuration settings:
    - SMGRB5800Admin user settings
    - SCEP settings
    - certificates settings
    - Web services settings

Also note that the User Rights feature is not integrated with System Manager. The User Rights feature is available only in the local IP Office Manager and is intended only for B5800 Branch Gateways that are not configured to be managed centrally through System Manager.

Chapter 10: Session Manager Configuration

This chapter provides procedures to configure Avaya Aura® Session Manager to support calls to and from B5800 Branch Gateway systems. Avaya Aura® System Manager R6.2 is used to administer Session Manager. Perform the following procedures:

1. View the SIP domains for which the Session Manager provides call management. Multiple domains can be listed. See Viewing the SIP domains on page 166.
2. Identify logical and/or physical locations where SIP entities reside. IP address patterns can be used to define different locations within the Avaya Aura® network, for example the IP address range of each B5800 Branch Gateway system. The creation of locations allows features such as bandwidth management to be applied to connections from those locations. See Creating locations on page 166.
3. Create a set of digit adaptations in order to ensure correct routing. If the digits to or from a branch need alteration in order to be routed correctly at either end, this can be done using a table of digit adaptations. Each SIP entity (branch) is associated with its own set of digit adaptations. See Creating adaptations on page 167.
4. Add each B5800 Branch Gateway system to the list of SIP entities that send calls to and from the Avaya Aura® network. See Creating SIP entities on page 167.
5. Add an entity link for each SIP entity including each B5800 Branch Gateway. An entity link must be added to define the ports and transport method used for connections between the SIP entity and the Session Manager. See Creating entity links on page 168.
6. Create time ranges to control when different routing policies are used. See Creating time ranges on page 169.
7. Add a routing policy. A routing policy consists of a selected SIP entity as its destination and a number of time ranges that define when the policy can be used. See Creating routing policies on page 169.
8. Add dial patterns. Dial patterns are used to match digits received to a destination. Each dial pattern has an associated routing policy that defines the target entity for matched calls and when the match should be used. See Creating dial patterns on page 170.

Note:

You must complete fields marked with an asterisk. Fields not marked with an asterisk are optional.

For more information about administering Session Manager, see “Chapter 5: Managing Session Manager routing” in *Administering Avaya Aura® Session Manager*, document number 03–603324.

Viewing the SIP domains

The domain for which the Session Manager is authoritative was added when Session Manager was initially configured for the B5800 Branch Gateway system. The domain name set in the B5800 Branch Gateway system's Session Manager line configuration (see Adding an Avaya Aura Session Manager line on page 145) should match one of the entries that is listed on the Domain Management page.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Domains**.

   The SIP domains are listed on the Domain Management page.

Creating locations

Locations are used to identify logical and/or physical locations where SIP entities reside. The location entries in Session Manager allow bandwidth management and call control to be applied for connections to and from those locations.

Typically locations are added for each B5800 Branch Gateway branch site.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Locations**.
3. On the Location page, click **New** to add a new location.
4. On the Location Details page, in the **Name** field, enter a name to identify the location.
5. In the **Notes** field, enter notes about the location, as appropriate.
6. In the **Managed Bandwidth Units** field, accept the default setting.
7. In the **Total Bandwidth** field, accept the default setting, blank.
8. In the **Multimedia Bandwidth** field, accept the default setting, blank.
9. For the **Audio Calls Can Take Multimedia Bandwidth** check box, accept the default setting, checked.
10. In the **Per-Call Bandwidth Parameters** section, accept the default settings.
11. In the **Alarm Threshold** section, accept the default settings.
12. In the **Location Pattern** section, click **Add** to add a location pattern.
13. In the **IP Address Pattern** field, enter an IP address pattern that matches the IP LAN address range.

The * character can be used as a match-all wildcard. For example, the pattern 192.168.42.* matches all addresses in the range 192.168.42.1 to 192.168.42.255.

14. In the **Notes** field, enter notes about this location pattern, as appropriate.
15. Click **Commit**.

Creating adaptations

Occasionally calls to or from the branch may require digit conversion in order to ensure correct routing. For example, reinserting an external dialing prefix. This is done using a set of digit conversions stored by the digit adaptation associated with the SIP entity.

Adaptations are optional and are deployment specific. For more information, see “Adaptations” in “Chapter 5: Managing Session Manager routing” in *Administering Avaya Aura®Session Manager*, document number 03-603324.

Creating SIP entities

A SIP entity is required for each branch system. This is in addition to the SIP entities that should already exist for Session Manager and Communication Manager or Communication Manager Feature Server or Evolution Server.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **SIP Entities**.
3. On the SIP Entities page, click **New** to create a new SIP Entity.
4. On the SIP Entity Details page, in the **Name** field, enter the name of the SIP entity.
5. In the **FQDN or IP Address** field, enter the IP address of the B5800 Branch Gateway system LAN interface configured for the Session Manager line operation.
6. In the **Type** drop-down box, select **SIP Trunk**. **SIP Trunk** is the correct selection for branches deployed in the distributed branch user model.
7. In the **Notes** field, enter a description to help identify this SIP entity, as appropriate.
8. In the **Adaptation** drop-down box, select the adaptation that contains the digit conversions to apply to calls to and from the location.
9. In the **Location** drop-down box, select the location that matches the location you configured in Creating locations on page 166.

10. In the **Time Zone** drop-down box, select the time zone for the location.
11. For the **Override Port & Transport with DNS SRV** check box, accept the default setting, unchecked.
12. In the **SIP Timer B/F (in seconds)** field, accept the default setting, 4.

    Note:

    If you see that calls are abnormally terminated, you should increase this number.
13. In the **Credential Name** field, accept the default setting, blank.
14. In the **Call Detail Recording** field, accept the default setting.
15. In the **SIP Link Monitoring** drop-down box, accept the default, **Use Session Manager Configuration**.
16. Click **Commit**.

Creating entity links

For each SIP entity communicating with the Avaya Aura® Session Manager, an entity link needs to be configured. That includes one for each B5800 Branch Gateway.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Entity Links**.
3. On the Entity Links page, click **New**.
4. In the **Name** field, enter a name to describe this link.
5. In the **SIP Entity 1** drop-down box, select the name of the Session Manager system that is at one end of the link.

   SIP Entity 1 must always be a Session Manager instance. For a Session Manager line from a B5800 Branch Gateway system, this should match the Session Manager set as the **SM Address** in the Session Manager line's configuration.
6. In the **Protocol** drop-down box, select **TCP**.

   When TCP is selected, the **Port** field is automatically set as **5060**. This is the port to which the SIP Entity 2 sends SIP requests.
7. In the **SIP Entity 2** drop-down box, select the name of the B5800 Branch Gateway system that is at the other end of the link.

   When you selected TCP in the previous step, the **Port** field was automatically set as **5060**.
8. Select the **Trusted** check box.

This check box must be checked. If it is not checked, calls from the associated SIP Entity 2 will be denied by Session Manager.

9. In the **Notes** field, enter notes regarding this entity link, as appropriate.
10. Click **Commit**.

Creating time ranges

Additional time ranges can be created and used with a routing policy to define when the routing policy is active. For most B5800 Branch Gateway implementations, you do not need to define additional time ranges. If you need to add or adjust a time range, see “Creating Time Ranges” in *Administering Avaya Aura Session Manager*, document number 03-603324.

Creating routing policies

A routing policy is a collection of multiple time ranges and a destination SIP entity. For each dial pattern configured to route calls received by the Session Manager, the routing policy associated with that dial pattern defines when and where matching calls are directed.

Separate routing policies are required for each B5800 Branch Gateway entity to which the Session Manager routes calls.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Routing Policies**.
3. On the Routing Policies page, click **New** to create a new routing policy.
4. On the Routing Policies Details page, in the **Name** field, enter a name to describe this routing policy.
5. For the **Disabled** check box, accept the default, unchecked.
6. In the **Notes** field, enter notes about this routing policy, as appropriate.
7. In the **SIP Entity as Destination** section, do the following:
    a. Click **Select**.
    b. On the SIP Entity List page, select the SIP entity to which the routing policy applies.
    c. Click **Select**.
8. Skip the **Time of Day** section, **Dial Patterns** section, and **Regular Expressions** section. You do not need to configure these settings.
9. Click **Commit**.

Creating dial patterns

A dial pattern is defined to direct calls prefixed with the branch prefix to each branch.

1. On the System Manager console, under **Elements**, click **Routing**.
2. In the left navigation pane, click **Dial Patterns**.
3. On the Dial Patterns page, click **New** to create a new dial pattern.
4. On the Dial Pattern Details page, in the **Pattern** field, enter the branch prefix.

   This is the dialed number or number prefix that the dial pattern is intended to match.
5. In the **Min** field, enter the minimum length (1 to 36) of the dialed number that the pattern should match. For example, if the branch prefix is 3 digits and the extension number length is 4 digits, you would enter 7.
6. In the **Max** field, enter the maximum length (1 to 36) of the dialed number that the pattern should match. For example, if you set this to the same value as the **Min** value, the dial pattern will match only internal calls.
7. For the **Emergency Call** check box, leave the check box set to the default setting, unchecked.
8. In the **SIP Domain** drop-down box, select the appropriate SIP domains that should be matched, or select **All** to allow calls from all SIP domains to be routed.
9. In the **Notes** field, enter notes to describe this dial pattern, as appropriate.
10. In the **Originating Locations and Routing Policies** section, click **Add**.
11. In the **Originating Location** section, click the check box for **Apply The Selected Routing Policies to All Originating Locations**.
12. In the **Routing Policies** section, click the check box for the routing policy that was created for the branch.
13. Click **Select**.
14. If you need to specify that calls from certain locations be denied, do the following:
    a. In the **Denied Originating Locations** section, click **Add**.
    b. Do one of the following:
       - Click the **Apply to All Originating Locations** check box.
       - Click the check box(es) for the locations that should be denied.
    c. Click **Select**.
15. On the Dial Patterns Detail page, click **Commit**.

Chapter 11: Voicemail configuration

This chapter provides the procedures to configure the voicemail system that the B5800 Branch Gateway will use. If Embedded Voicemail or Standalone Voice Mail are configured, see one of the following documents for information on how to configure user mailboxes, hunt group mailboxes, and auto attendants:

- *Implementing Embedded Voicemail for B5800 Branch Gateway Release 6.2*, document number 18-604098
- *Implementing Standalone Voice Mail for B5800 Branch Gateway Release 6.2*, document number 18-604088

Note:

Standalone Voice Mail must be installed on a separate Linux server.

Voicemail options

The B5800 Branch Gateway system uses its Embedded Voicemail by default. However, a number of other voicemail options are supported.

- **Embedded Voicemail** — Embedded Voicemail uses the system SD card in the B5800 Branch Gateway system control unit for storage of prompts and messages. Embedded Voicemail supports mailboxes for all local extension numbers, announcements to waiting callers, and auto attendants (up to 40) for external calls. Its capacity is limited to 15 hours of recorded messages, prompts and announcements. Embedded Messaging Port licenses must be purchased with sufficient quantity to support the configured number of ports.
- **Standalone Voice Mail** — Standalone Voice Mail provides the same features as Embedded Voicemail but with additional port capacity provided on a Linux server. You must have a Linux server installed to use this option. When you select this option, you must enter the IP address of the Linux server where Standalone Voice Mail is installed. This option provides a maximum capacity of 40 ports while the Embedded Voicemail option provides a maximum capacity of 6 ports. Embedded Messaging Port licenses must be purchased with sufficient quantity to support the configured number of ports.
- **Avaya Aura Messaging** — The B5800 Branch Gateway system can be configured to use Avaya Aura Messaging as its voicemail server when Session Manager is used as the core SIP router. See Configuring B5800 Branch Gateway to use Avaya Aura Messaging for voicemail on page 176 for more information. When Avaya Aura Messaging is used as the central voicemail system, at each branch you have the option to still use the local

Embedded Voicemail for auto attendant operation and for announcements to waiting calls. Note that for this configuration, Embedded Voicemail licenses are required.

- **Modular Messaging over SIP** — The B5800 Branch Gateway system can be configured to use Modular Messaging over SIP as its voicemail server when Session Manager is used as the core SIP router. See Configuring B5800 Branch Gateway to use Modular Messaging over SIP for voicemail on page 178 for more information. When Modular Messaging over SIP is used as the central voicemail system, at each branch you have the option to still use the local Embedded Voicemail for auto attendant operation and for announcements to waiting calls. Note that for this configuration, Embedded Voicemail licenses are required.

For more information about licensing, see Licensing on page 16.

About the Park and Page feature

Beginning with Release 6.2, B5800 Branch Gateway supports the Park and Page feature. Park and Page can be configured for a user's voicemail mailbox or for calls answered by the auto attendant. The Park and Page feature is available with Embedded Voicemail and Standalone Voice Mail. If Avaya Aura Messaging or Modular Messaging over SIP (the two central voice mail systems) are configured as the voicemail system with Embedded Voicemail or Standalone Voice Mail configured for auto attendant operation, the Park and Page feature can be configured for calls answered by the auto attendant.

The Park and Page feature allows a call to be parked while a page is made to a hunt group or extension. A caller can press a digit and the call is parked while an announcement is made to a paging zone, overhead paging system, or both. The page is repeated based on how the feature is configured until the parked call is picked up or the park timeout occurs. If the park timeout occurs, the caller hears the Park and Page error prompt and is then returned to the call flow that initiated the Park and Page and hears either the subscriber's personal greeting or the auto attendant main menu prompt.

The called party can use a short code or a programmed button on their phone to park and unpark incoming calls. For more information about short codes and button programming, see the Manager on-line help. The called party can also use the **Conference** button or the **Answer** soft key on their phone while the Page is occurring.

The procedure to configure Park and Page is provided in the following documents:

- *Implementing Embedded Voicemail for B5800 Branch Gateway Release 6.2*, document number 18-604098
- *Implementing Standalone Voice Mail for B5800 Branch Gateway Release 6.2*, document number 18-604088

Configuring Embedded Voicemail

About this task

Embedded Voicemail is the default voicemail configuration for B5800 Branch Gateway.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. In the **Voicemail Type** drop-down box, select **Embedded Voicemail**.

   Note:

   Fields applicable to this mode of voicemail support are enabled. If the field is not applicable, the field is disabled.
5. If you want the users to be presented with a display menu for access to their mailbox, check the **Messages Button Goes to Visual Voice** check box. For more information, see the IP Office Manager on-line help.
6. In the **Minimum Password Length** field, use the up and down arrows to set the appropriate minimum password length.
7. In the **Maximum Record Time** field, use the up and down arrows to set the maximum record time in seconds for recorded announcement and auto attendant prompts. messages and prompts.
8. In the **VoiceMail ports** field, use the up and down arrows to set the number of voicemail ports. This field must match the number of voicemail ports that are licensed for the system.
9. In the **Reception/Breakout (DTMF 0)** drop-down box, select the number to which a caller is transferred if they press **0** while listening to the mailbox greeting rather than leaving a message. Do one of the following:
   a. To configure Park and Page for this DTMF breakout, select **Park & Page** and then do the following:
      i. In the **Paging Number** drop-down box, select the appropriate hunt group or user extension.
      ii. In the **Retries** field, use the up and down arrows to set the number of times to repeat the page.

iii. In the **Retry timeout** field, use the up and down arrows to set the amount of time to elapse before the page is repeated. The time is set in 15–second increments.

b. To configure Centrex Transfer for this DTMF breakout, select **Centrex Transfer** and then enter the transfer number in the **Transfer Number** field.

c. To configure an extension number for this DTMF breakout, select the appropriate extension number from the **Reception/Breakout (DTMF 0)** drop-down box.

Note:

You can also enter an external number in this field.

10. For the **Breakout (DTMF 2)** drop-down box, repeat step 9.
11. For the **Breakout (DTMF 3)** drop-down box, repeat step 9.
12. In the **SIP Name** field, enter the appropriate name.
13. In the **SIP Display Name (Alias)** field, enter the appropriate name.
14. In the **Contact** field, enter the appropriate name.
15. Configure the **Anonymous** check box as appropriate. This feature is enabled when this check box is selected.

Note:

For more information about the fields in the SIP Settings section, see the IP Office Manager on-line help.

Configuring Standalone Voice Mail

About this task

The B5800 Branch Gateway system can be configured to use Standalone Voice Mail. Standalone Voice Mail provides additional port capacity provided on a Linux server. Before you perform this procedure, Standalone Voice Mail must be installed and configured on the Linux server. The Standalone Voice Mail server and required Linux operating system components are provided on the IP Office Applications DVD. For more information, see *Implementing Standalone Voice Mail for the Avaya B5800 Branch Gateway*, document number 18-604088.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.

2. In the left navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. In the **Voicemail Type** drop-down box, select **Standalone Voice Mail**.

   Note:

   Fields applicable to this mode of voicemail support are enabled. If the field is not applicable, the field is disabled.
5. If you want the users to be presented with a display menu for access to their mailbox, check the **Messages Button Goes to Visual Voice** check box. For more information, see the IP Office Manager on-line help.
6. In the **Voicemail IP Address** field, enter the IP address of the Linux server where Standalone Voice Mail is installed.
7. In the **Minimum Password Length** field, use the up and down arrows to set the appropriate minimum password length.
8. In the **Maximum Record Time** field, use the up and down arrows to set the maximum record time in seconds for recorded announcement and auto attendant prompts.
9. In the **VoiceMail ports** field, use the up and down arrows to set the number of voicemail ports. This field must match the number of voicemail ports that are licensed for the system.
10. In the **Reception/Breakout (DTMF 0)** drop-down box, select the number to which a caller is transferred if they press **0** while listening to the mailbox greeting rather than leaving a message. Do one of the following:
    a. To configure Park and Page for this DTMF breakout, select **Park & Page** and then do the following:
        i. In the **Paging Number** drop-down box, select the appropriate hunt group or user extension.
        ii. In the **Retries** field, use the up and down arrows to set the number of times to repeat the page.
        iii. In the **Retry timeout** field, use the up and down arrows to set the amount of time to elapse before the page is repeated. The time is set in 15–second increments.
    b. To configure Centrex Transfer for this DTMF breakout, select **Centrex Transfer** and then enter the transfer number in the **Transfer Number** field.
    c. To configure an extension number for this DTMF breakout, select the appropriate extension number from the **Reception/Breakout (DTMF 0)** drop-down box.
11. For the **Breakout (DTMF 2)** drop-down box, repeat step 10.
12. For the **Breakout (DTMF 3)** drop-down box, repeat step 10.
13. In the **SIP Name** field, enter the appropriate name.

14. In the **SIP Display Name (Alias)** field, enter the appropriate name.
15. In the **Contact** field, enter the appropriate name.
16. Configure the **Anonymous** check box as appropriate. This feature is enabled when this check box is selected.

Note:

For more information about the fields in the SIP Settings section, see the IP Office Manager on-line help.

Configuring B5800 Branch Gateway to use Avaya Aura Messaging for voicemail

About this task

The B5800 Branch Gateway system can be configured to use Avaya Aura Messaging as its voicemail server.

Note:

If Avaya Aura Messaging is used as the central voicemail system, you are able to still use the local Embedded Voicemail or Standalone Voice Mail for auto attendant operation and for announcements to waiting calls.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. In the **Voicemail Type** drop-down box, select **Avaya Aura Messaging**.

   Note:

   Fields applicable to this mode of voicemail support remain enabled.
5. To enable the local B5800 Branch Gateway system features for Embedded Voicemail auto attendants and announcements, in the **Use embedded for AA and Announcements** drop-down box, select the appropriate embedded voicemail. The announcements are those that the callers hear when the call in on hold.

Note:

You must also enable the announcements. Do this by selecting the check box for **Announcements On** which appears when you select **Hunt Group > Announcements** tab and **Users > Announcements** tab.

6. In the **AAM Number** field, enter the extension number configured for mailbox access to the Avaya Aura® Messaging system. Note that this number is automatically routed via the active Avaya Aura®Session Manager line. It does not need to be routed through the normal branch call routing.
7. In the **AAM PSTN Number** field, enter the PSTN number to which you want to reroute attempts to access mailboxes when the Avaya Aura®Session Manager line(s) are out of service. (This field is optional.)

   When calls to access voicemail are routed by this method, the calls go through the PSTN trunk that is configured on the B5800 Branch Gateway.

   Note:

   The PSTN voicemail number requires a corresponding Short Code entry so that the calls are routed to the correct line during rainy-day operation.
8. For the **Enable Voicemail Instructions Using DTMF** check box, do one of the following:

   a. To send the voicemail instructions as DTMF tones, ensure the **Enable Voicemail Instructions Using DTMF** check box is selected (that is, checked).

      When this check box is selected, the voicemail mail box number of the recipient and the appropriate digit(s), such as # or ## that are used to leave or collect a message, are automatically sent as DTMF tones so the caller does not need to enter those digits.

   b. To require the caller to dial the user's voicemail mail box to send the required DTMF digits, do not select this check box (that is, the check box is not checked).

      The capability to turn this feature off is provided because there may be networks where the DTMF digits may not correctly reach the messaging system due to a provider's network characteristics. When this feature is turned off, the DTMF digits are not automatically sent. Instead, the caller will dial the user's mail box number to manually send the required DTMF digits to access the mailbox.
9. In the **Maximum Record Time** field, use the up and down arrows to set the maximum recording length in seconds for recorded announcement and auto attendant prompts.

   Note:

   You can set a number in this field only if you selected one of the two voicemail options in the **Use embedded for AA and Announcements** drop-down box.

10. In the **VoiceMail Ports** field, use the up and down arrows to set the number of licensed voicemail ports.

    Note:

    You can set a number in this field only if you selected one of the two voicemail options in the **Use embedded for AA and Announcements** drop-down box. Avaya Aura Messaging requires SIP Trunk Session configuration and uses SIP Trunk Sessions licenses.

11. Accept the default setting (**on**, that is check box is checked) for **Enable Voicemail Instructions Using DTMF**.
12. Click **OK**.
13. Select **File > Save Configuration**.
    The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Configuring B5800 Branch Gateway to use Modular Messaging over SIP for voicemail

About this task

The B5800 Branch Gateway system can be configured to use Modular Messaging as its voicemail server.

Note:

If Modular Messaging over SIP is used as the central voicemail system, you are able to still use the local Embedded Voicemail or Standalone Voice Mail for auto attendant operation and for announcements to waiting calls.

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **System**.
3. Click the **Voicemail** tab.
4. In the **Voicemail Type** drop-down box, select **Modular Messaging over SIP**.

   Note:

   Fields applicable to this mode of voicemail support remain enabled.

5. To enable the local B5800 Branch Gateway system features for Embedded Voicemail auto attendants and announcements, in the **Use embedded for AA and Announcements** drop-down box, select the appropriate embedded voicemail. The announcements are those that the callers hear when the call in on hold.

   Note:

   You must also enable the announcements. Do this by selecting the check box for **Announcements On** which appears when you select **Hunt Group > Announcements** tab and **Users > Announcements** tab.

6. In the **MM Number** field, enter the extension number configured for mailbox access to the Modular Messaging system. Note that this number is automatically routed via the active Avaya Aura®Session Manager line. It does not need to be routed through the normal branch call routing.
7. In the **MM PSTN Number** field, enter the PSTN number to which you want to reroute attempts to access mailboxes when the Avaya Aura®Session Manager line(s) are out of service. (This field is optional.)

   This number needs to be a valid DID number from the branch to the Modular Messaging system. When calls to access voicemail are routed by this method, the caller will be prompted by Modular Messaging to indicate the action they are performing (leaving or collecting messages) and the target mailbox.

   Depending on the call routing being used by the branch system for external PSTN calls, you may need to do additional configuration to ensure that this number is routed via a branch PSTN trunk. See Modular Messaging and Avaya Aura Messaging PSTN Fallback on page 180 for more information.
8. In the **Maximum Record Time** field, use the up and down arrows to set the maximum recording length in seconds for recorded announcement and auto attendant prompts.

   Note:

   You can set a number in this field only if you selected one of the two embedded voicemail options in the **Use embedded for AA and Announcements** drop-down box.
9. In the **VoiceMail Ports** field, use the up and down arrows to set the number of licensed voicemail ports.

   Note:

   You can set a number in this field only if you selected one of the two voicemail options in the **Use embedded for AA and Announcements** drop-down box. Modular Messaging over SIP requires SIP Trunk Session configuration and uses SIP Trunk Sessions licenses.
10. Accept the default setting (**on**, that is check box is checked) for **Enable Voicemail Instructions Using DTMF**.
11. Click **OK**.

12. Select **File > Save Configuration**.
    The Send Configuration window appears and the Configuration Reboot Mode is set to **Immediate**. Do not change the reboot mode.

Modular Messaging and Avaya Aura Messaging PSTN Fallback

When the branch is configured to use Modular Messaging over SIP or Avaya Aura Messaging for its voicemail services, that configuration includes setting an internal Modular Messaging or Avaya Aura Messaging number (800700 for the following example) for calls to Modular Messaging or Avaya Aura Messaging which are automatically routed via the Session Manager line.

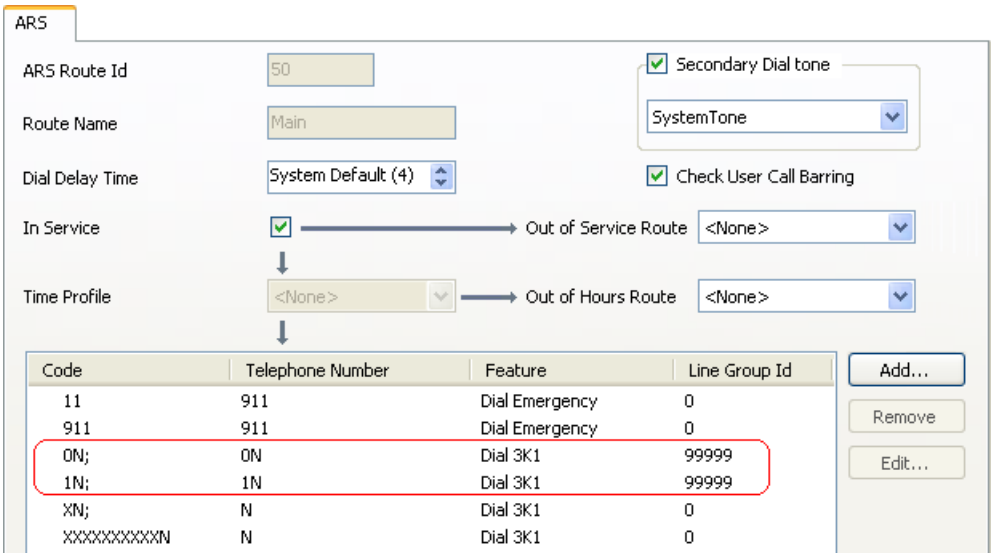
An additional Modular Messaging or Avaya Aura Messaging PSTN number can also be configured for use when the Session Manager line is not in service (915553800701 for the following example). However, it may also require additional configuration to ensure that this number is correctly routed to a branch PSTN trunk. That could be done using a system short code, but doing it in the ARS form keeps all the branch PSTN call routing in one place for ease of maintenance.

Adding an overriding short code

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **ARS**.

3. Click **50: Main**.



Within the ARS form, the default **1N;** short code is the one used for national calls. It would match the MM PSTN Number or AAM PSTN Number and attempt to route it to the SM Line which we know is out of service if the MM PSTN Number or AAM PSTN Number is being used for calls to voicemail. We can change the routing by adding a specific short code for the MM PSTN Number or AAM PSTN Number.

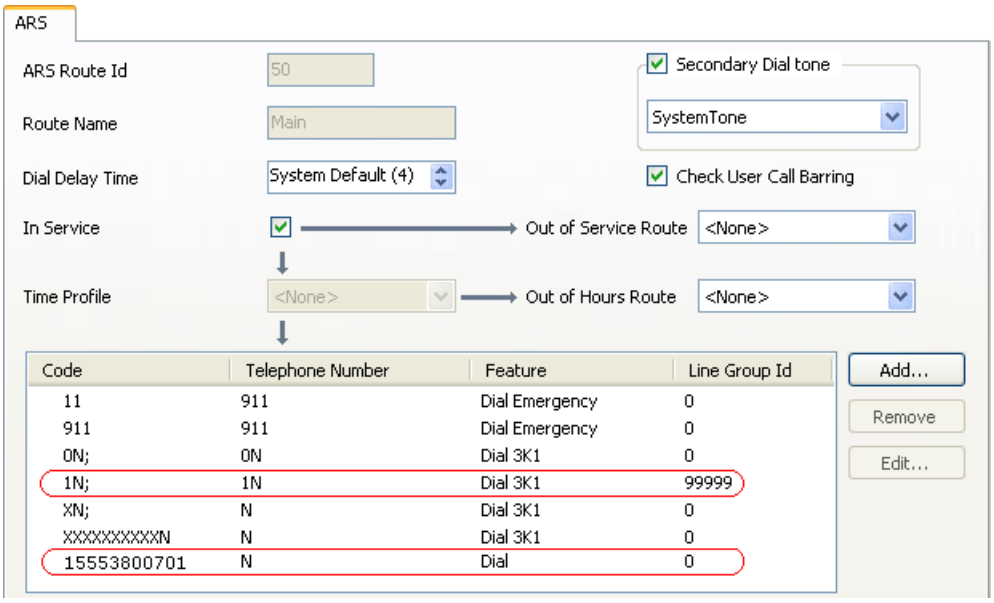
4. To add a short code, click the **Add...** button.
5. Make the changes as follows:
   a. In the **Code** field, set this to match the external PSTN number for Modular Messaging or Avaya Aura Messaging without the external dialing prefix.
   b. In the **Feature** drop-down box, select **Dial3K1**.
   c. In the **Telephone Number** field, set this to **N** to match the whole number in the **Code** field.

      Note:

      For a setup where the voicemail mail box numbers configured on Modular Messaging or Avaya Aura Messaging are the same as the caller's DID, the short code to route the PSTN call should be configured so that the caller ID is withheld. To do this, enter a `W` in the **Telephone Number** field of the short code. This ensures that during rainy-day operation, the voicemail system does not automatically go to the voicemail mail box of the caller based on the caller ID.

   d. In the **Line Group Id** drop-down box, select the line group ID being used for the branch's PSTN trunks. The default is 0.
6. Click **OK**.
   The ARS now has two short codes that will potentially match external national calls. However, one is a more exact match for certain calls and therefore will be applied

to those calls.



7. Click **OK**.
8. Select **File > Save Configuration**.

Uploading an auto attendant audio file

About this task

You are able to upload and convert audio files to System Manager that can be used in the B5800 Branch Gateway system configuration auto attendant feature. Once uploaded, from IP Office Manager you are able to select the audio files from the Auto Attendant page.

Note:

If you are using a system template, you can add the audio file to the template to push the audio file down to multiple B5800 Branch Gateway systems.

Procedure

1. From the System Manager console, under **Services**, select **Templates**.
2. On the Templates page, click **B5800 System Configuration**.
3. On the B5800 Branch Gateway System Configuration Templates page, under Templates List, select **More Options > Manage Audio**.
4. On the Manage Audio page, click the **Browse** button to locate the .wav file you want to upload.

5. Click the **Upload** button.
   The voice file is uploaded to System Manager in the .c11 format that is required for Embedded Voicemail on B5800 systems. The file is automatically converted from the .wav format to the .c11 format.
6. When finished, click the **Done** button.

Chapter 12: User administration

This chapter provides the procedures to add distributed users to B5800 Branch Gateway and Avaya Aura® System Manager.

Adding distributed users to System Manager

About this task

When you add a distributed user to System Manager, you must configure a B5800 Branch Gateway Profile on System Manager.

Procedure

1. On the System Manager console, under **Users**, click **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. On the User Management page, click **New**.
4. On the New User Profile page, in the Identity section, do the following:
   a. In the **Last Name** field, enter the user's last name.

      Note:

      Depending on how the branches and stations in your system are named and organized, you could enter a location name in this field, for example `Chicago 25`. Then in the next field, **First Name**, you could enter a location within that branch, for example `cashier`.
   b. In the **First Name** field, enter the user's first name.
   c. In the **Middle Name** field, enter the user's middle name.
   d. In the **Description** field, enter a description of this user profile.
   e. In the **Login Name** field, enter the extension user login in the format, username@domainname.com or extension@domainname.com. For example, nsmith@avaya.com or 5002432@avaya.com.

      For survivability mode operation with a B5800 Branch Gateway system, the user name without the domain name should match the user name configured in the branch system.
   f. In the **Authentication Type** drop-down box, accept the default setting, **Basic**.
   g. In the **Password** field, enter the password required to log into System Manager for personal web configuration.

h. In the **Confirm Password** field, enter the password again.
i. In the **Localized Display Name** field, enter the name to be used as the calling party.
j. In the **Endpoint Display Name** field, enter the user's full name.
k. In the **Title** field, enter the user's title if applicable.
l. In the **Language Preference** drop-down box, select the appropriate language.
m. In the **Time Zone** drop-down box, select the user's time zone.
n. In the **Employee ID** field, enter the user's employee ID.
o. In the **Department** field, enter the user's department.
p. In the **Company** field, enter the name of the user's company.
q. To add a postal address for this user, do the following:
    i. Expand the Address section.
    ii. Click **New**.
    iii. On the Add Address page, complete the fields as appropriate.
r. To add multiple phone numbers for this user, do the following:
    i. Expand the Phone Details section.
    ii. Complete the fields as appropriate.
    iii. Click **Add**.

5. To specify a localized language, expand the Localized Names section, and do the following:
    a. In the **Language** drop-down box, select the language for displaying the user name.
    b. In the **Display Name** field, enter the user's name.
    c. Click **Add**.
6. To add a TDM or IP endpoint, or a distributed SIP endpoint, such as an 11xx/12xx SIP phone, click the **Communication Profile** tab.
7. Accept the default values for the **Communication Profile Password** field, **Confirm Password** field, **Name** field, and **Default** check box.
8. Click the **B5800 Branch Gateway Endpoint Profile** check box, and do the following:
    a. In the **System** drop-down box, select the appropriate system.
    b. Check the **Use Existing Extension** check box if there is an available extension that you want to assign to this user.
    When you select this check box, if there are unassigned extensions, a drop-down box appears from which you can select an unassigned extension to assign to this user.
    c. In the **Extension** field, enter the appropriate extension.
    d. In the **Template** drop-down box, select the appropriate template.

When you select a template, the **Set Type** field is automatically populated based on the template selected.

e. To change other parameters such as call appearances or feature buttons for this user, click the **Endpoint Editor** button and do the following:

   i. Update the fields as appropriate.

   ii. Click **Save** to save your changes.

   iii. Click **Exit** to exit the Endpoint Editor.

   This updates parameters for this user. The changes are not reflected in the template.

   Note:

   Parameters for this user can also be configured using the endpoint template. See Creating an endpoint template on page 133 for more information.

f. For the **Delete Extension On User Delete** check box, do one of the following:

   - Accept the default, unchecked, if you are using an analog or digital set type template and this feature is checked for other set types.
   - Select this check box if you want the extension to be deleted when the extension is unassigned or the communication profile is deleted.

9. Click **Commit**.

   A distributed user is added on the B5800 Branch Gateway and is associated with a user in System Manager.

10. Repeat this procedure for each distributed user you want to add.

Editing the B5800 Branch Gateway Endpoint Profile for a user

About this task

Use this procedure to edit a B5800 Branch Gateway Endpoint Profile for a distributed user.

Procedure

1. On the System Manager console, under **Users**, click **User Management**.
2. In the left navigation pane, click **Manage Users**.
3. From the list of users on the User Management page, select the user you want to edit.
4. Click **Edit**.

5. Click the **Communication Profile** tab to expand that section.
6. Expand the **Communication Address** section.
7. Expand the **B5800 Branch Gateway Endpoint Profile**.
8. To change the extension for this user, in the **Extension** field enter the appropriate extension.
9. To apply a different template to this user, in the **Template** drop-down box, select the appropriate template.
10. To change other parameters for this user, click the **Endpoint Editor** button.
    IP Office Manager is launched where you can edit data for this user.
11. Update the fields as appropriate.
12. Click **Save**.
    You return to the edit user window in System Manager.
13. Click **Commit**.

Chapter 13: Managing license files with PLDS

PLDS Overview

The Avaya Product Licensing and Delivery System (PLDS) provides customers, Avaya Partners, distributors, and Avaya Associates with tools for managing license entitlements and electronic delivery of software and related license files. Using PLDS, you can perform operations such as license activations, license upgrades, license moves, and software downloads.

Installation software packages for Avaya products are available as ISO files on PLDS. Users can download the ISO images to a PC, and choose to either burn a DVD for installation or transfer the ISO file to the target server for installation.

Note:

The B5800 Branch Gateway R6.2 administrator applications are provided on DVD. They are not available for download from PLDS. However, once available, you will be able to download B5800 Branch Gateway R6.2 Service Packs from PLDS.

You can check PLDS to determine if a later service pack or software release is available. If updates do exist, see the appropriate upgrade procedures, contact Avaya, or contact the Avaya Partner Service representative.

When you place an order for a PLDS-licensed software product, the license entitlements on the order are automatically created in PLDS. Once these license entitlements are created, you receive an e-mail notification from PLDS. This e-mail notification includes a license activation code (LAC). Using the LAC, you can quickly find and activate the newly purchased license entitlements in PLDS. You can then download the license file.

Important:

You must provide the WebLM host ID to activate the license file in PLDS. The primary WebLM host ID is the MAC address of a physical network interface card (NIC) on the server.

If you are not using WebLM to manage the licenses, you must provide the host ID of each B5800 Branch Gateway in your network to generate a license for each branch. The host ID is the Feature Key Serial Number printed on the B5800 Branch Gateway System SD card. For more information, see Licensing on page 16.

Examples of license management tasks that you can perform in PLDS include:

- Adding more license entitlements to an existing activation
- Upgrading a license file to a new major release
- Moving license entitlement activations between license hosts
- Regenerating a license file with an new host ID

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) Web site at https://plds.avaya.com.
   The PLDS Web site redirects you to the Avaya single sign-on (SSO) Web page.
2. Log in to SSO with your SSO ID and password.
   The PLDS registration page is displayed.
3. If you are registering:
   - as an Avaya Partner, enter the Partner Link ID. If you do not know your Partner Link ID, send an e-mail to prmadmin@avaya.com.
   - as a customer, enter one of the following:
     - Company Sold-To
     - Ship-To number
     - License authorization code (LAC)
4. Click **Submit**.
   Avaya will send you the PLDS access confirmation within one business day.

About license activation

What is license activation?

License activation is a process of activating license entitlements by specifying a license host and host ID of the WebLM server. The process includes generating the license file.

Note:

If you are not using WebLM to manage the licenses, you must provide the host ID of each B5800 Branch Gateway in your network to generate a license for each branch. The host ID

is the Feature Key Serial Number printed on the B5800 Branch Gateway System SD card. For more information, see Licensing on page 16.

When license entitlements are activated, PLDS generates Activation Records containing the activation information and License/Key.

Types of license activation

Types of activation include:

- Regular activation: where license entitlements are activated to generate Activation Records.
- Upgrade activation, which involves either:
  - Activating license entitlements that have been marked as upgradeable. When you activate these license entitlements, you can generate License/Key for either the current version or the old version.
  - Activating upgrade license entitlements, which are purchased to upgrade other existing license entitlements. When users activate these license entitlements, they select the license entitlements to upgrade.

Activating license entitlements

Before you begin

You know the Host ID of the License Host if you are activating license entitlements on a new License Host.

About this task

Use the License Activation Code (LAC) to activate one or more license entitlements. You can activate all of the licenses, or you can specify a number of licenses to activate from the quantity available. Upon successful activation of the license entitlements, PLDS creates an Activation Record and sends an Activation Notification e-mail message to the customer who is registered with the entitlements. The Activation Record and Activation Notification provide details on the number of activated licenses and the License Host. The license file can be accessed on the License/Keys tab of the Activation Record in PLDS and is also an attachment to the Activation Notification e-mail message. You must install the license file on WebLM to use the licenses.

Note:

If you are not using WebLM to manage the licenses, you must install the license file on each B5800 Branch Gateway to use the licenses. For more information, see Licensing on page 16.

Procedure

1. Type `http://plds.avaya.com` in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.

3. In the **LAC(s)** field of the Quick Activation section, enter the LAC that you received in an e-mail message.

   Note:

   If you do not have an e-mail message with your LAC, follow the steps in the Searching for Entitlements section and make a note of the appropriate LAC from the LAC column.

   Note:

   The Quick Activation automatically activates all license entitlements on the LAC. However, you can remove line items or specify a number of licenses to activate from the quantity available.

4. Enter the License Host information.

   You can either create a new license host or use an existing license host.

5. Click **Next** to validate the registration detail.

6. Enter the License Host Information.

   The Host ID is the MAC address of the server hosting the WebLM server. The Host ID is obtained from the Server Properties page of the WebLM server where the license file will be installed.

   Note:

   If you are not using WebLM to manage the licenses, you would enter the Host ID of the B5800 Branch Gateway. This is the Feature Key Serial Number printed on the System SD card. You must add dashes between pairs of digits to provide the number in MAC address format (nn-nn-nn-nn-nn-nn). You can also get the Host ID from Manager. For more information, see Licensing on page 16.

7. Enter the number of licenses to activate.

8. Review the Avaya License Agreement and accept the agreement if you agree.

9. Perform the following steps to send an activation notification e-mail message:

   a. In the **E-mail to** field, enter e-mail addresses for any additional activation notification recipients.
   b. Enter any comments or special instructions in the **Comments** field.
   c. Click **Finish**.

10. Click **View Activation Record**.

    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From the **License/Key** tab, you can view and download the license

file. Install each license file on the WebLM server associated with the License Host.

Note:

For B5800 Branch Gateway, when using WebLM to manage licensing, a single license file is generated for all B5800 Branch Gateways in the multiple branches. A single license file is not generated for each branch or application. If you are not using WebLM to manage the licenses, individual license files are installed on a single branch at a time, where the branch is the License Host. For more information, see Licensing on page 16.

Searching for license entitlements

About this task

Use this functionality to search for an entitlement by using any one or all of the following search criteria:

- Company name
- Group name
- Group ID
- License activation code

In addition to these search criteria, PLDS also provides other additional advanced search criteria for searching license entitlements.

Note:

Avaya associate or Avaya Partners can only search license entitlements by company name.

Procedure

1. Type http://plds.avaya.com in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Click **Assets** > **View Entitlements**.

   The system displays Search Entitlements page.
4. To search license entitlements by *company name*, enter the company name in the **%Company: field**. To see a complete list of companies before searching for their corresponding entitlements, do the following:

   a. Click the **magnifying glass** icon.

b. Enter the name or several characters of the name and a wildcard (%) character.
c. Click **Search Companies**.
d. Select the desired company name from the list of options.

Tip:

You can use a wildcard (%) character if you do not know the exact name of the company you are searching for. For example, if you enter Av%, the system searches for all the company names starting with the letter Av. You can enter a wildcard character at any position in the search criteria.

5. To search license entitlements by *group name*, enter the appropriate information in the **%Group name:** or **%Group ID:** fields.

   Group Names or IDs are specific to Functional Locations and Sold-To's that define the actual location of equipment and software.

   Tip:

   You can use a wildcard character if you do not know the exact name of the group you are searching for. For example, if you enter Gr%, the system searches for all the groups starting with the characters Gr. You can enter a wildcard character at any position in the search criteria.

6. To search license entitlements by *LAC*, enter the specific LAC in the **%LAC:** field.

   Tip:

   You can use a wildcard character if you do not know the exact LAC you are searching for. For example, if you enter AS0%, the system searches for all the LACs starting with AS0. You can enter a wildcard character at any position in the search criteria.

   You will receive LACs in an e-mail if you have supplied the e-mail address to your sales order. If you do not have this code, search by using one of the other search criteria.

7. To search license entitlements by *application*, *product* or *license status*, select the appropriate application, product, and/or status from the field.
8. Click **Search Entitlements**.

Result

All corresponding entitlement records appear at the bottom of the page.

Moving activated license entitlements

Before you begin

Host ID or License Host name of the move from/to License Host.

About this task

Use this functionality to move activated license entitlements from one License Host to another. You can chose to move all or a specified quantity of license entitlements.

Note:

If you move a specified number of activated license entitlements from one host to another by using the Rehost/Move transaction in PLDS, two new license files are generated:

- One license file reduces the number of license entitlements on the License Host from which you are moving license entitlements.
- One license file increases the number of license entitlements on the License Host to which you are moving license entitlements.

Install each of these license files on the appropriate server.

If you move all activated license entitlements, only one license file is generated. Install this new license file on the License Host to which you are moving license entitlements. Remove the license file from the License Host from which you are moving all license entitlements.

Procedure

1. Type http://plds.avaya.com in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Click **Activation** > **Rehost/Move** from the Home page.
4. Click **View Activation Record information** to find and select licenses to rehost or move.

   You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.

   Note:

   If you are an Avaya associate or Avaya Partner, enter the search criteria and click **Search Activation Records**.
5. Select **Rehost/Move** for the License Host from which you are moving license entitlements.
6. In the **Search License Hosts** field, enter the License Host to which you are moving license entitlements.

Alternatively, you can click **Add a License Host** to select an existing License Host.

7. Validate the Registration Detail and click **Next**.
8. Enter the License Host Information.

   The Host ID is the MAC address of the server hosting the WebLM server. The Host ID is obtained from the Server Properties page of the WebLM server where the license file will be installed.

   Note:

   If you are not using WebLM to manage the licenses, you would enter the Host ID of the B5800 Branch Gateway. This is the Feature Key Serial Number printed on the System SD card. You must add dashes between pairs of digits to provide the number in MAC address format (nn-nn-nn-nn-nn-nn). You can also get the Host ID from Manager. For more information, see Licensing on page 16.
9. Enter the number of Licenses to move in the **QTY column** field and click **Next**.
10. Accept the Avaya Legal Agreement.
11. Perform the following steps to send an activation notification e-mail message:
    a. In the **E-mail to** field, enter e-mail addresses for any additional activation notification recipients.
    b. Enter any comments or special instructions in the **Comments** field.
    c. Click **Finish**.
12. Click **View Activation Record**.

    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.

      Note:

      For B5800 Branch Gateway, when using WebLM to manage licensing, a single license file is generated for all B5800 Branch Gateways in the multiple branches. A single license file is not generated for each branch or application. If you are not using WebLM to manage the licenses, individual license files are installed on a single branch at a time, where the branch is the License Host. For more information, see Licensing on page 16.

Regenerate License files

Use this functionality to regenerate the license file on a selected License Host. During the regeneration process, you can only modify host ID information.

Regenerating a license file

Procedure

1. Type http://plds.avaya.com in your Web browser to access the Avaya PLDS Web site.
2. Enter your Login ID and password to log on to the PLDS Web site.
3. Click **Activation** > **Regeneration** from the Home page.
4. Search License Activations to Regenerate.
   You can search the activation records by the Company name, license host, Group name or ID using the Search Activation Records functionality.
5. Click **Regenerate** from the appropriate record.
6. Validate the Registration Detail and click **Next**.
7. Validate the items that will regenerate and click **Next**.
8. Accept the Avaya Legal Agreement.
9. Perform the following steps to send an activation notification e-mail message:
   a. In the **E-mail to** field, enter e-mail addresses for any additional activation notification recipients.
   b. Enter any comments or special instructions in the **Comments** field.
   c. Click **Finish**.
10. Click **View Activation Record**.
    - The **Overview** tab displays a summary of the license activation information.
    - The **Ownership** tab displays the registration information.
    - The **License/Key** tab displays the license files resulting from the license activation. In general, a single license file will be generated for each application. From the **License/Key** tab, you can view and download the license file. Install each license file on the WebLM server associated with the License Host.

      Note:

      For B5800 Branch Gateway, when using WebLM to manage licensing, a single license file is generated for all B5800 Branch Gateways in the multiple

branches. A single license file is not generated for each branch or application. If you are not using WebLM to manage the licenses, individual license files are installed on a single branch at a time, where the branch is the License Host. For more information, see Licensing on page 16.

Chapter 14: Standalone SAL Gateway for remote service

Avaya Client Services (ACS) uses the Secure Access Link (SAL) Gateway to provide remote delivery of service to the B5800 Branch Gateway. The supported configuration requires a standalone SAL gateway that is deployed in the enterprise headquarters/data center and using the B5800 Branch Gateway administration applications — Manager, System Status, and System Monitor. See Administration software suite on page 77 for a description of these applications.

SAL Gateway R2.1 or higher software must be installed on a customer-provided server in the enterprise at a central location that allows for network connectivity to each deployed branch. The SAL Gateway manages the B5800 Branch Gateways in multiple branches, relaying alarms from the B5800 Branch Gateways back to Avaya, and proxying connection requests for support engineers. The SAL solution is fully customer controlled through the deployment and use of the optional SAL policy server.

Note:

System Platform's Virtual SAL Gateway (VSALGW) is not supported in managing each individual branch. The VSALGW is only officially supported by Avaya in management of system platform “on-board” devices such as System Platform, Session Manager and System Manager. Each B5800 Branch Gateway branch is considered an “off-board” device.

Use of SAL to access the B5800 Branch Gateway administration tools and System Manager

You are able to access the B5800 Branch Gateway administration tools and Avaya Aura® System Manager through SAL.

- **Manager**

  Manager is an administration tool used to configure and upgrade the B5800 Branch Gateway system. You can use Manager to administer each branch individually. You are able to use SAL to access the Manager application for local or remote configuration management of the B5800 Branch Gateway system.

  Note:

  For B5800 Branch Gateway upgrades and Embedded File Management, you must access Manager that is installed on a PC that resides within the customer network.

- **System Status Application**

System Status is an administration tool used to monitor the current status of individual branches in the B5800 Branch Gateway system. You are able to use SAL to access the System Status Application that is installed locally or remotely.

- **System Monitor** (Tier3/4 tool only)

  System Monitor is an administration tool that provides detailed traces of all activity on the B5800 Branch Gateway system.

  Note:

  You are able to use SAL to access the System Monitor application that is installed on a PC that resides within the customer network.

- **Avaya Aura System Manager**

  System Manager is a central management system that delivers a set of shared management services and a common console for System Manager and its components. System Manager provides a single access interface to administer multiple branch locations and multiple distributed or centralized B5800 Branch Gateway users.

For more information about the B5800 Branch Gateway administration tools and System Manager, see Management on page 14 and Administration software suite on page 77.

SAL Gateway installation and registration

To install SAL Gateway, see Chapter 2 in *Secure Access Link 2.1, SAL Gateway Implementation Guide*, document number 146775, which is available on the Avaya support Web site http://support.avaya.com. The *Secure Access Link 2.1 Gateway* software download is also available on the Avaya support Web site.

Registering a product with Avaya is a process that uniquely identifies the device so that Avaya can service it. A SAL Gateway registration form is provided with your software download. See Universal Install/SAL Registration Request Form on page 201 for more information. To register the SAL Gateway, complete Step 1 on the form and send it to salreg@avaya.com. The following information is requested in Step 1:

- Your company name
- Avaya Sold-to Number (customer number)
- Your contact information, so that Avaya can contact you if there are questions

Avaya uses this information to register your gateway. When the registration is complete, Avaya will send you an e-mail that provides the following information:

- The Solution Element ID and Product ID numbers
- A list of the devices currently registered at this location
- A list of other locations for your company

Note:

Optional: If you want to get Solution Element IDs (SEID) from other locations, complete the Step 2 tab of the registration sheet and send it to salreg@avaya.com using the link included on the sheet. Avaya will send you a list of SEIDs from the locations you selected.

B5800 Branch Gateway registration and SAL Gateway on-boarding

Each B5800 Branch Gateway deployed must be registered with Avaya. To add managed devices to your SAL Gateway using the Solution Element IDs (SEID) provided to you during SAL Gateway registration described above, see “Managed element configuration” in Chapter 4 in the *Secure Access Link 2.1, SAL Gateway Implementation Guide*, document number 146775, which is available on the Avaya support Web site.

When you have added all your managed devices, complete Step 2 of the SAL Gateway registration form for each managed device you added to your SAL Gateway and send the form to salreg@avaya.com. When this form is received, the Avaya registration team makes the appropriate changes to allow access to your managed devices through the SAL Gateway. Avaya will then confirm via an e-mail notification that remote access to your product has been enabled through your SAL Gateway.

B5800 Branch Gateway SAL-based alarming

The SAL Gateway supports alarming for the B5800 Branch Gateway managed device. You must change the alarm destination on your B5800 Branch Gateway managed device so that alarms are routed to your centralized SAL Gateway. See SNMP on page 224 for more information. During the registration and on-boarding process of each branch, the Avaya registration team also tests alarming through the SAL Gateway and back into Avaya alarm receivers.

Universal Install/SAL Registration Request Form

You can download this form from the Avaya support web site as follows:

1. Go to the Avaya support Web site http://support.avaya.com.
2. Select **More Resources** > **Equipment Registration**.

3. Under **Non-Regional (Product) Specific Documentation**, select **Universal Install/SAL Registration Request Form**.
4. Complete the registration form as instructed.

Chapter 15: Additional system procedures

This chapter provides procedures for ongoing maintenance and management of your system, such as system shutdown and reboot, replacing components, and system backup.

Changing the IP address settings

About this task

Use this procedure to change the system name, IP address, IP mask, or DHCP settings of the B5800 Branch Gateway system. By default the B5800 Branch Gateway system name is set to match its MAC address. The system name can be changed to something more distinctive. For more information about the system default settings, see Default configuration on page 85. Note that if you change the IP address settings, you must restart the system.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. On the **System** tab, in the **Name** field, enter a distinctive name for this B5800 Branch Gateway system.
4. Click **OK**.
5. Click the **LAN1** tab.
6. On the **LAN Settings** sub-tab, do the following:
   a. Change the IP Address to match the customer requirements.
   b. Change IP Mask to match the customer requirements.
   c. Change DHCP Mode setting to match the customer requirements.

   These settings are used for the **LAN** port on the back of the control unit.
7. Click **OK**.
8. Click the **LAN2** tab.
9. On the **LAN Settings** sub-tab, do the following:
   a. Change the IP Address to match the customer requirements.
   b. Change IP Mask to match the customer requirements.
   c. Change DHCP Mode setting to match the customer requirements.

   These settings are used for the **WAN** port on the back of the control unit.

10. Click **OK**.
11. Select **File > Save Configuration**.
12. Reboot the system.

Default passwords

Do not change any other settings than those described below until you have read and understood the B5800 Branch Gateway Security Mode feature. See the IP Office Manager online help for more information. From IP Office Manager, click the **Help** button in the lower-right section of the window. Then in the left navigation pane, in the **Contents** tab, select **Security Mode**.

Changing the security settings

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. Select **File** > **Advanced** > **Security Settings**.
3. In the Select IP Office window, click the check box for the appropriate system.
4. Click **OK**.
5. In the Security Service User Login window, enter a user name and password of an account that has security configuration access to the B5800 Branch Gateway system.

   The defaults are **security** and **securitypwd**.
6. In the left navigation pane, click **System**.
7. Click the **Unsecured Interfaces** tab.

   The password in the **System Password** field is used by Manager for remote software upgrade of the B5800 Branch Gateway system. The default password is **password**.
8. Next to the **System Password** field, click the **Change** button.
9. Enter a new password and click **OK**.
10. Click **OK**.
11. Click on **Service Users**.

The list shows the service user accounts that can access the system configuration. The default service users Administrator, Manager and Operator each use the same value (Administrator, Manager and Operator) as their password.

12. For each of these service users:
    a. Click on the service user name.
    b. In the **Service User Details** tab, click on **Change** and enter a new password.
    c. Click **OK**.
    d. Click **OK**.
13. Click on **General**.

    The general security settings are displayed in the main display area.
14. Next to the **Password** field, click on **Change** and enter a new password for the security administrator.
15. Click on **File** > **Configuration** to exit security configuration mode and return to the B5800 Branch Gateway configuration.

Changing the remote user password

About this task

The B5800 Branch Gateway configuration contains a user whose password is used as the default for remote dial-in access to the B5800 Branch Gateway network. Use this procedure to change this user's password.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **User**.
3. In the user list, click **RemoteManager**.
4. On the **User** tab, do the following:
    a. In the Password field, enter a new password for the user.
    b. In the Confirm Password field, enter the new password again.
5. Click **OK**.
6. Select **File > Save Configuration**.

System shutdown

B5800 Branch Gateway systems can be shut down in order to perform maintenance. The shut down can be either indefinite or for a set period of time after which the B5800 Branch Gateway will automatically reboot. During the shut down process, the current configuration in the control unit's RAM memory is copied to the System SD card.

Warning:

- A shutdown must always be used to switch off the system. Simply removing the power cord or switching off the power input may cause errors.
- This is not a polite shutdown, any users calls and services in operation will be stopped. Once shutdown, the system cannot be used to make or receive any calls until restarted.
- The shutdown process takes up to a minute to complete. When shutdown, the CPU LED and the base card LEDs 1 and 9 (if trunk daughter card fitted) will flash red rapidly. The memory card LEDs are extinguished. Do not remove power from the system or remove any of the memory cards until the system is in the this state.
- To restart a system when shutdown indefinitely, or to restart a system before the timed restart, switch power to the system off and on again.

Shutting down the system using Manager

Procedure

1. Start Manager.
2. Select **File** > **Advanced** > **System Shutdown**.
   The Select IP Office window appears.
3. Select the B5800 Branch Gateway system you want to shut down.
   The System Shutdown Mode window appears.
4. Do one of the following:
   - To shut down the system for an indefinite period of time, select **Indefinite**.

     To restart the system you must switch the power off and then on.
   - To shut down the system for a specific period of time, select **Timed** and then specify the duration in hours and minutes.

     The system will automatically reboot after the set time has elapsed.

5. Click **OK**.

Shutting down the system using the System Status application

Procedure

1. Start System Status and access the system status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Shutdown System**.
4. Select the time duration for the shutdown or indefinite.

Shutting down the system using a system phone

About this task

To shut down the system using a system phone, you must be administered as a System Phone user. You can shut down the system using a 1400, 1600, or 9600 series phone (excluding XX01, XX02, and XX03 models). Unlike Manager, a system phone user cannot select an indefinite shutdown. A system phone user can set a timed shut down of between 5 minutes and 24 hours. Your Login Code is used to restrict access to some system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **System Shutdown**.
4. Select a time period for the shutdown. It must be in between 5 minutes and 24 hours.
5. Select **Done** and then **Confirm** to begin the shutdown.

Shutting down the system using the AUX button

Procedure

On the control unit, press the **AUX** button for more than 5 seconds.

The control unit will shutdown with the restart timer set to 10 minutes.

Rebooting the system

About this task

You can use Manager to reboot an B5800 Branch Gateway system.

Procedure

1. Start Manager.
2. Select **File** > **Advanced** > **Reboot**.
3. In the Select B5800 window, select the B5800 Branch Gateway system.
4. Enter your user name and password.
5. In the Reboot window, do one of the following:
   - Select **Immediate** to reboot the system immediately.
   - Select **When Free** to reboot the system when there are no calls in progress. This selection can be combined with the **Call Barring** options.
   - Select **Timed** and then specify a time in hours and minutes.

     This reboots the system the same as When Free but first waits for a specific time. After the specified time, the system waits for there to be no calls in progress and then reboots. This selection can be combined with the **Call Barring** options.

     Note:

     If the time is after midnight, the system's normal daily backup is canceled.
6. In the **Call Barring** section, select **Incoming Calls** and/or **Outgoing Calls**. These settings are used when the reboot mode is **When Free**. They bar the sending or receiving of any new calls.
7. Click **OK**.

About changing components

Except for memory cards, cards and external expansions modules must only be removed and added to an B5800 Branch Gateway system when the system is turned off. See Memory card removal on page 259 and System shutdown on page 206 for more information.

Note that for extension ports, by default both an extension entry and a user entry are configured in the system. Extension entries can be deleted without deleting the corresponding user entry. This allows retention of the user settings and association of the user with a different extension by changing that extension's Base Extension number to match the user's Extension ID.

In the following procedures, the term component refers to a card fitted into the control unit or an external expansion module.

Replacing a component with one of the same type

About this task

If you are replacing a component with one of the same type and capacity, no configuration changes are required.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 206.
2. Remove the card or external expansion module.

   Note:

   The card slot or expansion port used as the replacement must be installed in the same position.
3. Install the replacement using the appropriate procedure for the type of component. See Base and trunk card installation on page 59 or Connecting external expansion modules on page 70 for more information.
4. Restart the B5800 Branch Gateway system.

Replacing a component with one of higher capacity

About this task

If you are replacing a component with one of the same type but with higher capacity, when restarted the B5800 Branch Gateway system will automatically create configuration entries for the new trunks or extensions/users.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 206.
2. Remove the card or external expansion module.

   Note:

   The card slot or expansion port used as the replacement must be installed in the same position.
3. Install the replacement using the appropriate procedure for the type of component. See Base and trunk card installation on page 59 or Connecting external expansion modules on page 70 for more information.
4. Restart the B5800 Branch Gateway system.
5. Use Manager to configure the new trunks or extension/users.

Replacing a component with one of lower capacity

About this task

If you are replacing a component with one of the same type but with lower capacity, when restarted the B5800 Branch Gateway system configuration must be edited to remove redundant entries.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 206.
2. Remove the card or external expansion module.

   Note:

   The card slot or expansion port used as the replacement must be installed in the same position.
3. Install the replacement using the appropriate procedure for the type of component. See Base and trunk card installation on page 59 or Connecting external expansion modules on page 70 for more information.

4. Restart the B5800 Branch Gateway system.
5. Use Manager to delete the trunks or extensions/users in the configuration that are no longer supported by the replacement component.

Replacing a component with one of a different type

About this task

If you are replacing a component with one of a different type, you must perform two procedures; one to permanently remove the component and then one to add the component.

Procedure

1. Remove the existing component. See Permanently removing a component on page 212.

   Note:

   Be sure to reboot the system and edit the configuration after you remove the component.

2. Install the new component. See Adding a new component on page 211.

Adding a new component

About this task

If you are adding a new component to an available slot or port, when restarted the B5800 Branch Gateway system will automatically create configuration entries for the new trunks or extensions/users.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 206.
2. Install the new component using the appropriate procedure for the type of component. See Base and trunk card installation on page 59 or Connecting external expansion modules on page 70 for more information.
3. Restart the B5800 Branch Gateway system.
4. Use Manager to configure the new trunks or extension/users.

Permanently removing a component

About this task

If you are permanently removing a component, when restarted the B5800 Branch Gateway system configuration must be edited to remove redundant entries.

Procedure

1. Turn the B5800 Branch Gateway system off. See System shutdown on page 206.
2. Remove the card or external expansion module.
3. Restart the B5800 Branch Gateway system.
4. Use Manager to delete the trunks or extensions/users in the configuration that relate to the component removed.
5. In the **Control Unit** section of the configuration, delete the entry for the component that is no longer present in the system.

Swapping extension users

About this task

This procedure explains how to swap extensions for two users. This example refers to User A and User B which represent any two users for whom you want to swap extensions.

Procedure

1. Load the B5800 Branch Gateway configuration.
2. Select **Extension**.
3. In the **Extension** section of the window, select the extension for User A.
4. In the **Base Extension** field, change the extension to User B's extension.

   Note:

   If Manager is set to validate edits, a warning appears that says this change conflicts with the existing Base Extension setting of another extension. Ignore the warning at this stage. Click **OK**.
5. In the **Extension** section of the window, select the extension for User B.
6. In the **Base Extension** field, change the extension to User A's extension.
7. Save the configuration back to the B5800 Branch Gateway system.

8. At each of the extensions, dial the log out short code set on the B5800 Branch Gateway system. The default is ***36**.
9. If either user is configured for **Forced Login**, they will have to complete the login process at their new extension using their Login Code.

About changing extension numbers

The default configuration for a new B5800 Branch Gateway system numbers each extension in sequence, going by module and port order, starting from 201. An extension entry is created in the configuration and also an associated user entry. A similar process occurs when a new extension expansion module is detected.

Important:

Extension versus User: It is important to understand that "extension number" is a user setting that belongs to and moves with the user. For example, a user can login at any phone and that phone then temporarily assumes the user's extension number and settings until they log off. The **Base Extension** value set for extensions in the B5800 Branch Gateway configuration indicates the default associated user of the extension. It is not the extension number of that port.

Renumbering all extensions and users

About this task

Use this procedure to shift all user extension numbers up or down by a set amount. Any settings linked to those numbers are adjusted including extension Base Extension settings. It does not affect hunt group extension numbers.

Warning:

This procedure alters extension settings and therefore requires a system reboot when the configuration is sent to the B5800 Branch Gateway.

Procedure

1. Select **Tools** > **Extension Renumber**.
2. In the Renumber window, in the **Value** field, enter the amount by which you want to shift the current extension numbering of extensions and users.
3. Click **Add** or **Subtract** as appropriate.
4. Click **OK**.

5. Send the configuration back to the B5800 Branch Gateway and select the appropriate settings for the reboot.

Changing a user's extension number

Procedure

1. Select **User**.
2. Select the relevant user.
3. On the **User** tab, in the **Extension** field, change the extension number to the new number.
4. Click on another field.

   If an error warning appears it is most likely due to a conflict with an existing use of that extension number. Do one of the following:

   - Click **Cancel** to return the user to their original extension number.
   - If you are planning to change the other extension number, click **OK** and then edit the other entry.

     Manager automatically propagates the number change to any hunt groups, incoming call routes, user buttons, bridged appearance buttons and call coverage appearance buttons associated with the user's original extension number.

     If the user has an extension with which they are associated by being the extension's **Base Extension** setting, that setting is not automatically updated. If the user should still be associated with that extension by default, the extension must be updated manually to match the user's new extension number.
5. To update the user's Base Extension setting, select **Extension**.
6. On the **Extn** tab, in the **Base Extension** field, change the base extension number to match the user extension who should now be associated with that extension port by default.
7. Click **OK**.

   Note:

   If a validation error message appears due to a user being associated with two extensions, ignore the message until all the user moves have been completed.
8. Repeat steps 2 through 7 for each user whose extension number you need to change.

9. Click ✓ to revalidate the configuration and check that there are no conflicts between users and associated extensions.
10. Send the configuration back to the B5800 Branch Gateway and select appropriate settings for the reboot.

Creating a backup of the system configuration using IP Office Manager

About this task

Before performing an upgrade, ensure you have a current backup of the B5800 Branch Gateway system configuration. If you do not, use this procedure to create a backup of the system configuration.

Procedure

1. Start Manager.
2. Select **File > Open Configuration**.
3. In the Select B5800 Branch Gateway window, select the appropriate system.
4. Click **OK**.
5. Enter the name and password for a service user account on that system.
6. Click **OK**.
   A BOOTP entry for the system is created in Manager. This also confirms communication between the Manager PC and the B5800 Branch Gateway system.
7. Select **File** > **Save Configuration As...** and save a copy of the configuration file onto the PC.

Creating a backup of the system configuration using System Manager

About this task

When you perform a backup of the system configuration from System Manager, the backup is stored on the local B5800 Branch Gateway. To store the system configuration backup on the System Manager server, you must synchronize the B5800 Branch Gateway with System

Manager. See Synchronizing B5800 Branch Gateway with System Manager on page 162 for more information.

Procedure

1. From the System Manager console, under **Elements**, select **B5800 Branch Gateway**.
2. In the left navigation pane, click **Backup and Restore**.
3. On the B5800 Branch Gateway Backup and Restore page, select the B5800 Branch Gateway device for which you want to create a backup.
4. Click **Backup**.
5. Do one of the following:
   - Click **Now** to run the backup job now.
   - Click **Schedule** to run the backup job at a scheduled date and time.

Upgrades using IP Office Manager

IP Office Manager includes software files for control units, external expansion modules and phones appropriate to the system's software level. The B5800 Branch Gateway system can be upgraded in two ways using IP Office Manager that is connected directly to the B5800 Branch Gateway system. These methods are:

- Using the IP Office Manager upgrade wizard. See Using the upgrade wizard on page 217.
- Using the System SD card. See System upgrade using the System SD card on page 256.

B5800 Branch Gateway systems can also be upgraded using Avaya Aura® System Manager. This method is used for systems that have already been upgraded from R6.1 to R6.2 and is used when multiple branches require upgrades. For more information, see Upgrading an R6.2 system with an R6.2 service pack on page 97.

Note:

Check the latest B5800 Branch Gateway Technical Bulletin for the B5800 Branch Gateway software release before proceeding any further. It may contain information relating to changes that occurred after this document was completed. Bulletins are available from http://support.avaya.com

- **Multiple Managers** — If more than one copy of Manager is running it is possible for the B5800 Branch Gateway system to request BIN files from a different Manager from the

one that started the upgrade process. Ensure that only one copy of Manager is running when upgrading an B5800 Branch Gateway system.

- **Other B5800 Branch Gateway applications** — Upgrading the core software of the B5800 Branch Gateway control unit may require upgrades to associated software. Typically B5800 Branch Gateway is compatible with the previous release of most B5800 Branch Gateway applications. However, for each B5800 Branch Gateway core software release, there may be exceptions. See the Technical Bulletin for the B5800 Branch Gateway core software release for more information.

Using the upgrade wizard

About this task

Before using the upgrade wizard, be sure you have a current backup of the system configuration. See Creating a backup of the system configuration using IP Office Manager on page 215 for more information.

Procedure

1. Start Manager.
2. Select **File** > **Advanced** > **Upgrade**.
3. Click the check box for the appropriate system.
4. Click **Upgrade**.
   The UpgradeWiz scans for B5800 Branch Gateway modules using the address specified in the **Unit/Broadcast Address** field.
5. If the expected control units are not shown, adjust the address in the **Unit/Broadcast Address** field, and click **Refresh**.

   The current version of each B5800 Branch Gateway .bin file held in the control units memory is displayed. This is regardless of whether that .bin file is currently being used by any module in the system.

   In the **Available** column, Manager lists the versions of software it has available. If Manager detects that there is a higher version available, the check box for that row is automatically selected.
6. Click the check box for the modules you want to upgrade.
7. Click the check box for **Validate**.

   When this option is selected, the upgrade wizard checks the amount of free RAM memory available in the control unit to temporarily store the new bin files. If insufficient memory is available, you will be prompted whether to continue with an off-line upgrade or cancel upgrading. If offline is selected, the system is rebooted into offline mode. It may be necessary to use the **Refresh** option within the upgrade wizard to reconnect following the reboot. Validate upgrade can then be attempted again to check the amount of available RAM memory for transfer of bin files. If the

memory is still insufficient, the option is offered to either do an unvalidated upgrade or cancel.

During a validated upgrade, the bin files required are transferred to the system and stored in temporary memory. The backup system files and upload system files actions are performed. Once all file transfers are completed, the upgrade wizard promps whether it is okay to proceed with the upgrade process. Select **Yes** to continue. Each module being upgraded will delete its existing core software, restart and load the new software file that was transferred. This process may take several minutes for each unit.

8. Select the following options as appropriate:
   - Click the check box for **Backup System Files** if, before upgrading to the new software, you want the current files in the System SD cards **/primary** folder copied to a **/backup** folder.
   - Click the check box for **Upload System Files** if you want the full set of software files that Manager has to be copied to the **/primary** folder on the System SD card. In addition to control unit and module software this will include phone software files. Following the reboot, the phone will upgrade using those files if necessary.
   - Click the check box for **Restart IP Phones** if you want all Avaya IP phones to be restarted following the upgrade and reboot. This will cause them to recheck whether the firmware they currently have loaded matches that on their configured file server. Use this option if the B5800 Branch Gateway system is the file server and the upgrade included new IP phone firmware.
9. Click **Upgrade**.
   The system password for each system is requested.
10. Enter the system password and click **OK**.

Restoring the system configuration using System Manager

Procedure

1. From the System Manager console, under **Elements**, select **B5800 Branch Gateway**.
2. In the left navigation pane, click **Backup and Restore**.
3. On the B5800 Branch Gateway Backup and Restore page, select the B5800 Branch Gateway device whose backup configuration you want to restore. You can select multiple devices.

4. Click **Restore**.
5. On the B5800 Branch Gateway Restore page, do one of the following:
    - Click **System Configuration** to restore the respective system configurations available in System Manager to the B5800 Branch Gateway device. The configuration you restore is the latest configuration available in System Manager.
    - Click **User** to restore the respective users from System Manager to the B5800 Branch Gateway device.
    - Click **System Configuration and Users** to restore the respective system configurations and users from System Manager to the B5800 Branch Gateway device.
    - Click **Restore Backup Stored on Devices** to restore the locally backed up configuration to the B5800 Branch Gateway device.
6. Do one of the following:
    - Click **Now** to perform the restore activity now.
    - Click **Schedule** to perform the restore activity at a scheduled date and time.

External output port (EXT O/P)

The B5800 Branch Gateway control unit is equipped with an external output port. The port is marked as EXT O/P and is located on the back of the control unit adjacent to the power supply input socket.

The port can be used to control up to two external devices such as door entry relay switches. The usual application for these switches is to activate relays on door entry systems. However, as long as the criteria for maximum current, voltage and if necessary protection are met, the switches can be used for other applications.

The switches can be switched closed, open or pulsed (closed for 5 seconds and then open). This can be done in a number of ways:

- Using B5800 Branch Gateway short codes.
- Through the Door Release option in B5800 Branch Gateway SoftConsole.

Default short codes: The following are the default short codes in the B5800 Branch Gateway configuration for external output switch operation. They use the short code features Relay On (closed), Relay Off (open) and Relay Pulse.

State	Switch 1	Switch 2
Closed	*39	*42

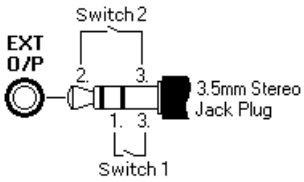
State	Switch 1	Switch 2
Open	*40	*43
Pulse	*41	*44

EXT O/P connections

EXT O/P ports use a standard 3.5mm stereo jack plug for connection. The B5800 Branch Gateway is able to open (high resistance), close (low resistance) or pulse (close for 5 seconds and then open) two switches within the port. Either switch can be operated separately. These switches are intended for activation of external relays in systems such as door opening systems.

⚠ Caution:

In installations where this port is connected to a device external to the building, connection must be via a towerMAX SCL/8 Surge Protector and a protective ground connection must be provided on the B5800 Branch Gateway control unit.

EXT O/P	Pin	Description
	1	Switch 1
	2	Switch 2
	3	0 Volts (Ground/Chassis)

- Switching Capacity: 0.7A
- Maximum Voltage: 55V d.c
- On state resistance: 0.7 ohms
- Short circuit current: 1A
- Reverse circuit current capacity: 1.4A
- Ensure that pins 1 and 2 are always at a positive voltage with respect to pin 3

3.5mm stereo audio jack plugs are frequently sold as pre-wired sealed modules. It may be necessary to use a multi-meter to determine the wiring connections from an available plug. Typically 3 (common to both relays) is the cable screen.

Example of BRI So8 module configuration

The ports on a BRI So8 module can be used for the connection of ISDN devices. Following are examples of how to configure a port on the BRI So8 module for an ISDN terminal and for video conferencing.

Example 1: ISDN terminal

About this task

In this example, calls on DID 123456 are routed to the first port of the So8 expansion module. That port has been configured as Line Group ID 701.

Procedure

1. Configure an incoming call routing. The destination is a short code that directs the call to the line group ID that contains the SO lines.

   The Bearer Capability has been set to **Any** to allow data and voice via this route.

   - Line Group ID: 0
   - Incoming Number: 123456
   - Destination: 123456
   - Bearer Capability: Any

2. Create a system short code. This is the destination used in the incoming call route.

   - Short Code: 123456
   - Telephone Number: 123456
   - Line Group ID: 701
   - Feature: Dial

3. Send the configuration to the control unit.
   Any call coming into the main system on DID 123456 will now be passed directly to the first port.

4. If you wish to assign DIDs from your main pool to individual ports and avoid network charges when dialing between them, try variations on the following:

   a. You have DID ranges, for example: 7325551000 to 7325551099. You wish to assign 7325551000-19 to port 1 and 7325551020-20 to port 2 etc.

b. Configure incoming call route. The # is used here instead of "n" to avoid problems with "Main". The minus sign means the number is processed from the left and so will wait for the whole number.
    - Line Group ID: 701
    - Incoming Number: -100x
    - Destination: #
c. Repeat for Line Group ID 702 etc.
d. Create short codes, for example:
    - Short Code: 100x
    - Telephone Number:
    - Line Group ID: 701
    - Feature: Dial

S0 calls dialed without the area code are handled locally without network charges. Calls with area calls will go via the network.

Example 2: video conference

About this task

In this example, calls are routed to a Polycom Viewstation module connected to a S0 port of the B5800 Branch Gateway system.

The following settings were used on 4 incoming data channels of a PRI line:

- Line Number: 5
- Channel Allocation: 23 -> 1
- Switch Type: 5ESS
- Line Sub Type: PRI
- Provider: AT&T
- Channels: 1-4
- Incoming Line Group: 95
- Outgoing Line Group: 95
- Direction: Bothway
- Bearer: Data
- Service: Accunet (this is a important)
- Admin: In Service

To route an incoming video call on the PRI lines configured above to an So8 module requires the following:

Procedure

1. Create a dial short code that has the SO port as its destination line group. For this example the following is used:
   - Short Code: 1500
   - Number:
   - Feature: Dial
   - Line Group: 601 (the So8 port number)
2. Create an incoming call routing that routes the appropriate calls to that short code. For this example the following is used:
   - Line Group: 95 (identifies calls using the PRI lines configured above)
   - Destination: 1500 (the short code created above)
   - Bearer: Any
3. To allow the video device on the S0 port to make outgoing calls to the PRI lines also requires a short code. For this example the following is used:
   - Code: 91N;
   - Number: N
   - Feature: Dial
   - Line Group: 95

   Polycom Video module settings

   The Polycom modules used in the previous example were the Viewstation 128, Viewstation 256 and Viewstation MP.

   The Polycom module must have software that supports 'Standard ETSI ISDN' (European ISDN) and have its ISDN Switch Protocol setting set to 'Standard ETSI Euro-ISDN'

   The following were the settings used during testing:

Characteristics	Admin/Software and Hardware/ Software
• Polycom View Station 512 MP • NTSC UIS Interface • View Station PVS 1419	• Software: 7.0.1 • Network Interface: S/T Interface • ISDN Version: IEUS v18:a00320
Admin/General Setup	**Admin/Video Network/ISDN Video Network**

Characteristics	Admin/Software and Hardware/ Software
• Country: USA • Language: English (USA) • Auto Answer: Yes • AllowDial: Yes • Allow User Setup: Yes • Maximum Time on Call: 480	• Country Code: 1 • Area Code: 732 • Number A: blank • Number B: blank • ISDN Switch Protocol: Standard ETSI Euro-ISDN
User Setup	**Admin/Video Network/IMUX**
• Auto Answer: Yes • PIP: Auto • Far Control of Near Camera: Yes • MP Mode: Auto	• Numbers: blank • SPID: blank • Audio Quality: 168KB/s • Advanced Dialing: Dial Channels in Parallel
System Information	**Admin/Software and Hardware/ Hardware**
• Release: 7.0.1 • Model: VS: 512	• Camera: NTSC • Video Comm Interface: ISDN_Quad_BRI • Network Interface Type: S/T Interface
Admin/Video Network	**Admin/Video Network/Call Preference**
• MultiPoint Setup: Auto	• ISDN Video Calls (H:320): Yes

SNMP

SNMP (Simple Network Management Protocol) is a standard network protocol that allows the monitoring and management of data devices across a network. An SNMP agent can be built into network devices such as routers and hubs. An SNMP manager application, for example CastleRock or HP OpenView, can then communicate with those devices.

B5800 Branch Gateway supports SNMP communication. This communication can be:

- **Polling:** Some SNMP applications (called "managers") send out polling messages to the network. They then record the responses of any SNMP enabled devices (called "agents").

This allows the application to create a network map and to raise an alarm when devices previously present do not respond.

- Most SNMP manager applications can also do simple IP address polling to locate non-SNMP enabled devices. However this method of polling does not identify the device type or other information.
- SNMP polling including details about the responding device. For example an B5800 Branch Gateway control unit's response includes the control unit type, level of software, routing table information, up time, etc.

- **Traps:** When certain events occur, a devices SNMP agent can send details of the event to the SNMP manager. This is called an SNMP trap. These appear in the event log of the SNMP manager. Most SNMP managers can be configured to give additional alerts in response to particular traps.
- **Management:** Some SNMP agents support device management and configuration changes through the SNMP manager interface. This is not supported by B5800 Branch Gateway.

B5800 Branch Gateway SNMP operation has been tested against Castle Rock SNMPc-EE 5.1.6c and HP OpenView Network Node Manager 6.41.

What information is available via SNMP

As described above, SNMP information can either be polled by the SNMP application or received as the result of the B5800 Branch Gateway sending SNMP trap information.

While the MIB files should not be edited, they can be read using a text editor and contain descriptions of all the various information objects that can be polled or sent and the information that each object will include. For a list of the MIB files, see Installing the B5800 Branch Gateway MIB files on page 225. The NOTIFICATION-TYPE objects are those used for SNMP traps. The other types of objects are those that can be polled.

Installing the B5800 Branch Gateway MIB files

To allow full communication between an SNMP agent and an SNMP manager, the SNMP manager must load MIB files (Management Information Base) specific to the SNMP agent device and the features it supports. These MIB files contain details of the information the agent can provide and the traps that it can send.

The MIB files for B5800 Branch Gateway operation are included on the B5800 Branch Gateway DVD in the folder **\AdminCD\smnp_mibs**. The actual files required and the method of loading depend on the SNMP manager application being used. The details below cover the two SNMP manager applications supported.

HP OpenView Network Node Manager

Procedure

1. Copy the following MIB files to the application's MIB folder.

MIB File	Source
rfc2737-entity-mib.mib	snmp_mibs\standard folder on OpenView Install CD.
avayagen-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on B5800 Branch Gateway Admin DVD.
ipo-prod-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on B5800 Branch Gateway Admin DVD.
ipo-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on B5800 Branch Gateway Admin DVD.
inet-address-mib.mib	\AdminCD\snmp_mibs\Standard folder on B5800 Branch Gateway Admin DVD.
rfc2213-integrated-services-mib.mib	\AdminCD\snmp_mibs\standard folder on OpenView Install CD.
diffserv-dscp-tc.mib	\AdminCD\snmp_mibs\Standard folder on B5800 Branch Gateway Admin DVD.
diffserv-mib-hpov.mib	\AdminCD\snmp_mibs\Standard folder on B5800 Branch Gateway Admin DVD.
ipo-phones-mib.mib	\AdminCD\snmp_mibs\IPOffice folder on B5800 Branch Gateway Admin DVD.

2. Start the OpenView Network Node Manager console.
3. Select **Options** and then Load/Unload MIBs: SNMP.
4. Select **Load** and select all the MIB files listed above.
5. Select **Compile**.

Castlerock SNMPc 5.1.6c and earlier

Procedure

1. Copy the following MIB files to the application's MIB folder. This folder is typically C:\Program Files\SNMPc Network Manager\mibfiles.

MIB file	Source
ENTITY-MIB	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
AVAYAGEN-MIB.mib	\AdminCD\snmp_mibs\IPOffice on B5800 Branch Gateway Admin DVD.
IPO-PROD-MIB.mib	\AdminCD\snmp_mibs\IPOffice on B5800 Branch Gateway Admin DVD.
IPO-MIB.mib	\AdminCD\snmp_mibs\IPOffice on B5800 Branch Gateway Admin DVD.
INET-ADDRESS-MIB.mib	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
INTEGRATED-SERVICES-MIB	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
DIFFSERV-DSCP-TC.mib	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
DIFFSERV-MIB.mib	\AdminCD\snmp_mibs\Standard on B5800 Branch Gateway Admin DVD.
IPO-PHONES-MIB.mib	\AdminCD\snmp_mibs\IPOffice on B5800 Branch Gateway Admin DVD.

2. In SMNPc select **Config > MIB Database**.
3. Select **Add** and select the MIB files listed above in the order listed.

Castlerock SNMPc V5.0.1

Procedure

1. Copy all of the B5800 Branch Gateway MIBs and standard MIBs from the B5800 Branch Gateway Administrator Applications DVD to the SNMPc mibfiles directory.
2. In the SNMPc mibfiles directory open the files STANDARD.mib and SNMPv2-SMI.mib in Notepad.

3. In the SNMPv2-SMI.mib file find the definition of zeroDotZero and copy this to the clipboard.
4. In the STANDARD.MIB file find the SNMPv2-SMI section and paste in the definition of zeroDotZero from the clipboard before the end of this section (just before the END statement).
5. Save the modified STANDARD.MIB file.
6. Add the MIB file SNMP-FRAMEWORK-MIB.mib to the MIB database.
7. Add all the MIB files in the order listed.
8. Compile the MIBs ready for use.

Note:

The IPO-PHONES-MIB.mib relies upon the DIFFSERV-MIB.mib for the definition of the textual convention of IndexInteger. The DIFFSERV-MIB needs the definition of the textual convention zeroDotZero which is normally defined in SNMPv2-SMI.mib. However including SNMPv2-SMI.mib in the MIB file compilation list results in errors due to conflicts with what appear to be internal definitions within SNMPc and the SNMPv2-SMI section in its STANDARD.mib file. Therefore to resolve the issue the required definition of zeroDotZero must be placed in the SNMPv2-SMI section in SNMPc's STANDARD.mib file.

Enabling SNMP and polling support

About this task

In order for the B5800 Branch Gateway control unit to be discovered and polled by an SNMP manager, its SNMP agent must be enabled and placed in the same read community as the SNMP manager.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **System Events** tab.
4. Select **SNMP Enabled**.
5. In the **SNMP Port** field, enter the UDP port number used by the SNMP agent to listen for and respond to SNMP traffic.

   The default is 161.
6. In the **Community (Read-only)** field, enter the community to which the device belongs for read access.

   This community name must match that used by the SNMP manager application when sending requests to the device. The community public is frequently used to

establish communication and then changed (at both the SNMP agent and manager ends) for security.

7. Click **OK**.
8. Select **File > Save Configuration** to send the configuration back to the B5800 Branch Gateway and then select **reboot**.
   After the reboot, the SNMP manager will be able to discover the control unit. The discovery includes the control unit type and the current level of core software.

Enabling SNMP trap sending

About this task

Use this procedure to configure the SAL Gateway as a trap destination. A maximum of 5 SNMP management stations can be configured as B5800 trap destinations. System Manager must be configured as a trap destination. When the Initial Installation Utility is used, System Manager is automatically configured as a trap destination. See Using the Initial Installation Utility on page 121 for more information.

Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **System**.
3. Click the **System Events** tab.
4. In the **Configuration** sub-tab, in the **SNMP Agent** section, ensure the **SNMP Enabled** check box is selected.
5. In the **Community (read-only)** field, enter the SNMP community name to which the system belongs.

   This community name must match that used by the SNMP manager application when sending requests to the device. The community public is frequently used to establish communication and then changed (at both the SNMP agent and manager ends) for security.
6. In the **SNMP Port** field, accept the default.
7. In the **Device ID** field, enter the alarm ID or PID of the registered system.

   Note:

   This enables product alarming back to Avaya via the Secure Access Link (SAL). The unique alarm ID is included in the var-bind of all SNMP trap notifications sent by the system. The alarm ID, or PID, is parsed out of the alarm and used for automatic case creation by matching the registered system's customer record with the alarm event.
8. In the **Contact** field, enter contact information as appropriate.

9. In the **Location** field, enter location information as appropriate.
10. Click the **Alarm** tab.
11. Click **Add**.
12. In the **New Alarm** section, do the following:
    a. Click the **Trap** option button.
    b. In the **IP Address** field, enter the IP address of the PC running the SNMP manager application.
    c. In the **Port** field, enter the port on which the trap messages should be sent.

       This is the UDP port on which the B5800 Branch Gateway sends SNMP trap messages. The default is 162.
    d. In the **Community** field, enter the community that will be used by the agent and the SNMP manager.
13. In the **Events** section, click the check boxes for the events you want to send.

    See the Manager on-line help for a description of the events.
14. Click **OK**.
15. Select **File > Save Configuration** to send the configuration back to the B5800 Branch Gateway and then select **reboot**.

DTE port maintenance

The DTE port on the back of control unit is not normally used when configuring an B5800 Branch Gateway system. However, in extreme cases, the DTE port can be used to default the system's configuration or to erase the core software if necessary.

⚠ Warning:

The procedures in this section should only be performed if absolutely necessary to return a system back to working order. In all cases, you must have a backup copy of the system configuration before you perform these procedures. See Creating a backup of the system configuration using IP Office Manager on page 215.

The DTE ports on B5800 Branch Gateway expansion modules are not used for any maintenance or diagnostics.

RS232 DTE port settings

The RS232 DTE ports are located on the rear of all control units and external expansion modules. The DTE ports on external expansion modules are not used. The RS232 DTE ports

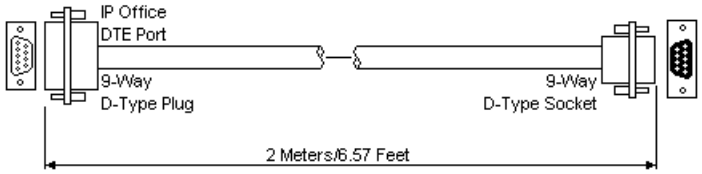
on the control units can be used for system maintenance and connection of serial terminal adaptors.

An asynchronous terminal program such as HyperTerminal is also required. Configure this for operation via a PC serial port, as follows:

Bits per second	38,400	**Parity**	None	**Flow Control**	None
Data bits	8	**Stop Bits**	1	**Settings** > **Emulation**	TTY

DTE cables

These cables are used for system maintenance and diagnostics under Avaya guidance. They can also be used for connection of RS232 serial terminal adaptor equipment to the control unit. This cable is a "Straight through DB9 female to DB9 male serial cable."



9-Way RS232 DTE Port	Signal	PC/Terminal Adaptor
3	⬅Receive data	3
2	➡Transmit Data	2
7	⬅RTS (Request To Send)	7
8	➡CTS (Clear To Send)	8
6	➡DSR (Data Set Ready)	6
5	●Ground	5
1	➡DCD (Data Carrier Detect)	1
4	⬅DTR (Data Terminal Ready)	4
9	➡RI (Ring Indicator)	9

About erasing the configuration

The following procedures erase the B5800 Branch Gateway configuration stored in the control unit. This includes both the current configuration being used in RAM memory and the backup configuration stored in non-volatile memory. Following this, the B5800 Branch Gateway will restart with a default configuration.

These procedures should be performed from a PC with a fixed IP address, directly connected to the B5800 Branch Gateway control unit and with the B5800 Branch Gateway system disconnected from any network. The control unit IP address will default to 192.168.42.1.

Important:

Do not perform any of these processes unless absolutely necessary. The configuration settings can be returned to the default settings using Manager by selecting **File** > **Advanced** > **Erase Configuration** command.

Erasing the configuration via debug

About this task

This procedure erases the system's configuration settings but does not alter the security settings. It is easier to use than the boot loader method. Before you perform this procedure, be sure you have a current backup of the system configuration. See Creating a backup of the system configuration using IP Office Manager on page 215 for more information.

Procedure

1. Attach the serial cable between the PC and the DTE port on the control unit.
2. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 230. Within a HyperTerminal session, the current settings are summarized across the base of the screen.
3. Enter `AT` (upper case).

   An `OK` response appears.
4. Enter `AT-DEBUG`.

   The time and date and then the `Hello>` prompt appears to show the system is ready to accept commands.
5. To erase the current configuration in RAM memory, enter `eraseconfig`.

   The `Hello>` prompt reappears.
6. To erase the backup configuration stored in non-volatile Flash memory enter **erasenvconfig**.

   The `Hello>` prompt reappears.
7. To reboot the system, enter `reboot`.

   The system reboots and restarts with a defaulted configuration.
8. Close the terminal program session.

9. Use Manager to edit and then upload an old configuration file or receive and edit the system's now defaulted configuration.

Erasing the configuration and security settings via the boot loader

About this task

This procedure erases the system's configuration settings and the security settings and resets them to the default settings. Before you perform this procedure, be sure you have a current backup of the system configuration. See Creating a backup of the system configuration using IP Office Manager on page 215 for more information.

Procedure

1. Attach the serial cable between the PC and the DTE port on the control unit.
2. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 230. Within a HyperTerminal session, the current settings are summarized across the base of the screen.
3. Arrange the program windows so that the terminal program and Manager TFTP log are visible at the same time.
4. Switch off power to the control unit.
5. Power on the control unit and press the escape key every second until you get a loader message. An example of this message is:

   ```
   P12 Loader 2.4
   CPU Revision 0x0900
   ```
6. Enter `AT` (upper case).

   An `OK` response appears. If `OK` does not appear, check the settings of your terminal program.
7. To erase the alarm log, enter `AT-X1`.
8. To erase the backup configuration stored in non-volatile memory, enter `AT-X2`.
   An `OK` response appears.
9. To erase the current configuration in RAM memory, enter `AT-X3`
   A series of `OK` responses appear.
10. Switch power to the control unit off and then back on.

    Messages appear as the control unit performs the start-up tasks.
11. Close the terminal program session.

12. Use Manager to edit and then upload an old configuration file or receive and edit the system's now defaulted configuration.

Resetting the security settings to the default settings

About this task

This procedure resets the systems security settings back to the default settings but does not alter the configuration settings.

Procedure

1. Attach the serial cable between the PC and the DTE port on the control unit.
2. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 230. Within a HyperTerminal session, the current settings are summarized across the base of the screen.
3. Enter `AT` (upper case).

   An `OK` response appears. If `OK` does not appear, check the settings of your terminal program.
4. Enter `AT-SECURITYRESETALL`.
   You are prompted to confirm the control unit's MAC address.
5. Enter the MAC address.
   An `OK` response appears.
6. Close the terminal program session.
7. Use Manager to edit the system's now defaulted security settings.

Resetting the configuration and security settings to the default settings via the boot loader

About this task

This procedure erases the system's configuration settings and the security settings and resets them to the default settings. Before you perform this procedure, be sure you have a current backup of the system configuration. See Creating a backup of the system configuration using IP Office Manager on page 215 for more information.

Procedure

1. Attach the serial cable between the PC and the DTE port on the control unit.
2. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 230. Within a HyperTerminal session, the current settings are summarized across the base of the screen.
3. Arrange the program windows so that the terminal program and Manager TFTP log are visible at the same time.
4. Switch off power to the control unit.
5. Power on the control unit and press the escape key every second until you get a loader message. An example of this message is:

   ```
   P12 Loader 2.4

   CPU Revision 0x0900
   ```
6. Enter `AT` (upper case).

   An `OK` response appears. If `OK` does not appear, check the settings of your terminal program.
7. To erase the backup configuration stored in non-volatile memory, enter `AT-X2`.
   An `OK` response appears.
8. To erase the current configuration in RAM memory, enter `AT-X3`
   A series of `OK` responses appear.
9. Switch power to the control unit off and then back on.

   Messages appear as the control unit performs the start-up tasks.
10. Close the terminal program session.
11. Use Manager to edit and then upload an old configuration file or receive and edit the system's now defaulted configuration.

About erasing the operational firmware

When the firmware loaded by the control unit is erased, the control unit begins making BOOTP requests for a replacement firmware file. Manager can act as a BOOTP server and respond to the control units request with the appropriate file from those installed with Manager.

When the firmware loaded by the B5800 Branch Gateway control unit is erased, the control unit will first look for replacement firmware on the System SD card before falling back to using a BOOTP request to Manager.

The procedure should be performed from a PC with a fixed IP address, directly connected to the B5800 Branch Gateway control unit and with the B5800 Branch Gateway system disconnected from any network. During the process, the control unit's IP address may default to a value in the 192.168.42.1 to 192.168.42.10 range. If this occurs it may be necessary to amend the BOOTP entry in Manager to match the address the system is using.

Important:

- Do not erase the core software unless absolutely necessary. The B5800 Branch Gateway software can normally be upgraded using Manager.
- These procedures erase the operational software. Before performing these procedures, you must know the MAC and IP addresses of the system, plus have a system backup and the correct .bin file for the control unit type and level of software.
- The presence of any firewall blocking TFTP and or BOOTP will cause these procedures to fail.

Erasing the core software via debug

Procedure

1. Start Manager.
2. In the **BOOTP** entries, check that there is an entry that matches the MAC address, IP address and .bin file used by the system. An entry is normally automatically created when a configuration has been loaded from the B5800 Branch Gateway system.
3. If an entry is not present, do the following:
   a. Create a new entry manually. The MAC address and IP address can be found in the control unit settings in the configuration file.
   b. Close Manager.
   c. Restart Manager.
4. Under **File** > **Preferences** ensure that Manager is set to 255.255.255.255. Also check that **Enable BootP Server** is checked.
5. Select **View** > **TFTPLog**.
6. Check that the required .bin file is present in Manager's working directory.
7. Attach the serial cable between the PC and the DTE port on the control unit.
8. Start the terminal program on your PC.

Note:

Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 230. Within a HyperTerminal session, the current settings are summarized across the base of the screen.

9. Enter `AT` (upper case).

   An `OK` response appears.

10. Enter `AT-DEBUG`.

    The time and date and then the `Hello>` prompt appears to show the system is ready to accept commands.

11. To erase the current configuration in RAM memory enter `upgrade`.
    The B5800 Branch Gateway system erases the current software and then sends out a BOOTP request on the network for new software. Manager responds and starts transferring the software using TFTP.

Erasing the core software via the boot loader

Procedure

1. Start Manager.
2. In the **BOOTP** entries, check that there is an entry that matches the MAC address, IP address and .bin file used by the system. An entry is normally automatically created when a configuration has been loaded from the B5800 Branch Gateway system.
3. If an entry is not present, do the following:
   a. Create a new entry manually. The MAC address and IP address can be found in the control unit settings in the configuration file.
   b. Close Manager.
   c. Restart Manager.
4. Under **File** > **Preferences** ensure that Manager is set to 255.255.255.255. Also check that **Enable BootP Server** is checked.
5. Select **View** > **TFTPLog**.
6. Check that the required .bin file is present in Manager's working directory.
7. Attach the serial cable between the PC and the DTE port on the control unit.
8. Start the terminal program on your PC.

   Note:

   Ensure that the DTE port settings are configured as described in RS232 DTE port settings on page 230. Within a HyperTerminal session, the current settings are summarized across the base of the screen.

9. Arrange the program windows so that the terminal program and Manager TFTP log are visible at the same time.
10. Switch off power to the control unit.
11. Power on the control unit and press the escape key every second until you get a loader message. An example of this message is:

    ```
    P12 Loader 2.4

    CPU Revision 0x0900
    ```

12. Enter `AT` (upper case).

    An `OK` response appears. If `OK` does not appear, check the settings of your terminal program.

13. Enter `AT-X`.
    Multi-Sector Erase response appears. The control unit then requests the .bin file that is stored on the System SD card.
14. If the files do not appear to be transferring, check that the IP address shown in the TFTP log matches the BOOTP entry. Adjust the BOOTP entry if necessary.
    When the file transfers are completed, the system reboots.

Reset button

The **Reset** button is on the control unit. Pressing the button while the control unit is starting up will pause the start up until the button is released. The effect of pressing the button during normal operation will depend on how long the button is pressed and is indicated by the CPU LED.

Press Duration (seconds)	CPU LED	Action	Summary
0 to 5	Off	None	None
5 to 10	Orange	Reboot when free	Reboot when free with new incoming/outgoing call barring. A reboot using the reset button is recorded in the audit trail.
10 to 30	Flashing orange	Erase configuration/ immediate reboot	Erase the configuration, alarm log and audit trail. Immediate reboot without waiting for active calls to end. See About erasing the configuration on page 231 for more information.
30 to 40	Red	Erase all	Erase configuration, alarm log and core software. See About

Press Duration (seconds)	CPU LED	Action	Summary
			erasing the operational firmware on page 235 for more information.
Over 40	Flashing green	None	None

Creating a WAN link

About this task

This procedure is a high level procedure for creating a data link from Site A to Site B via the WAN ports. For this example the IP address is 192.168.43.1.

Procedure

1. At Site A, on IP address 192.168.43, create a normal service.

   The service name can be any text and is used to identify this particular service. The account name and password entered for the service are presented to the remote end, therefore must match the user name and password configured at Site B. The Encrypted Password option can only be used if the remote end also supports CHAP.

2. Create a user.

   Under the **Dial In** tab, select **Dial In On**. This User account is used to authenticate the connection from the Site B. Note that if the service and user have the same name these two configuration forms are automatically linked and become an Intranet service. The user password is displayed at the bottom of the Service tab as the Incoming Password.

3. Setup RAS.

   If CHAP is to be used on this link, then the Encrypted Password option must be checked in the service and in the RAS service. The name of the RAS service must match the name of the service at Site B. Note that if the RAS settings are given the same name as the service and user they are automatically linked and become a WAN service. Ensure that the Encrypted Password option is not checked when using a WAN service.

4. Edit the WAN port.

   Do not create a new WAN port. The WAN port is automatically detected. If a WAN port is not displayed, connect the WAN cable, reboot the control unit and receive the configuration. The WAN port configuration form should now be added.

5. Create an IP Route.

   In the **IP address** field enter the network address of the remote end — *not* the IP address of the control unit. Under **Destination** select the service created above.

6. At Site B, on IP address 192.168.43, repeat steps 1 through 5 but alter the details to create a route from Site B to Site A.

Chapter 16: SD card management

There are two SD card slots in the control unit. They are labeled **System SD** and **Optional SD**.

Note:

For B5800 Branch Gateway, the System SD card must be a B5800 Branch Gateway System SD card. You cannot use an IP Office SD card in the System SD card slot on a B5800 Branch Gateway device. For more information, see “B5800 Branch Gateway System SD card” under System components on page 20.

System SD card slot

- An Avaya System SD card must be present in this slot at all times. This card holds copies of the B5800 Branch Gateway firmware and configuration and is used as the control units non-volatile memory.
- Each System SD card has a unique Feature Key serial number which is used for generating and validating licenses entered into the B5800 Branch Gateway configuration.
- The card stores the prompts for Embedded Voicemail operation and acts as the message store for embedded voicemail messages.
- Prior to any planned shutdown or restart of the B5800 Branch Gateway system, the current configuration running in the system's RAM memory is copied to the primary folder on the System SD card and to the systems non-volatile memory.
- Following a restart, the software in the primary folder is loaded by the control unit. If the required software is not present or valid, a sequence of fallback options is used, see Booting from the SD Cards on page 244 for more information.
- Following a restart, the configuration file, if present, in the primary folder is loaded by the control unit. If no file is present the system will check for a file in its internal non-volatile memory. If no copy is found it will generate a default configuration file. See Booting from the SD Cards on page 244 for more information.
- Once each day (approximately between 00:00 and 00:30) the B5800 Branch Gateway will copy the current configuration running in its RAM memory to the primary folder on the card.
- Configuration changes made using Manager are first written to the copy of the configuration file on the card and then merged with the configuration running in the system's RAM memory.
- The write lock setting on cards in the System SD card slot is ignored.

Optional SD card slot

- A card does not have to be present in this slot for normal B5800 Branch Gateway operation. The slot can be used for various maintenance actions.
- A card with updated B5800 Branch Gateway software or configuration can be inserted into the Optional SD card slot and those files are then transferred to the System SD card in order to upgrade the B5800 Branch Gateway system.
- The full contents of the System SD card can be copied to the Optional SD card while the B5800 Branch Gateway system is running.
- The write lock setting on cards in the Optional SD card slot is honored.

⚠ Warning:

Memory cards should always be shut down before being removed when the system is running. Though the card slot LEDs indicate when data is being written to a card, lack of flashing LEDs is not a sufficient safeguard. Shutting down the card will disable embedded voicemail if being used. If the System SD card is removed, features licensed by the card's Feature Key serial number will continue operating for up to 2 hours.

Card maintenance

Using Manager, the System Status application, or a phone configured as a system phone, you can perform the following procedure on the SD cards.

Procedure	Description	Manager	System Status	System Phone	Minutes
Backing up the primary folder using Manager on page 249	Copy the files in the primary folder on the System SD card to the/backup folder on the card.	✓	✓	✓	6
Restoring from the backup folder using Manager on page 250	Copy the files in the backup folder on the System SD card to the primary folder on the card and restart the B5800 Branch Gateway system.	✓	✓	✓	6
Backing up to the Optional SD card using Manager on page 252	Copy all the files on the System SD card to the Optional SD card.	✓	✓	✓	90
Upgrading using an Optional SD card on page 258	Copy the configuration file in the primary folder on the Optional SD card to the primary folder on the System SD card and then restart the B5800 Branch Gateway system.	✓	–	–	15
Upgrading remotely using	Upload a set of B5800 Branch Gateway software and embedded voicemail prompts to the System SD card.	✓	–	–	40

Procedure	Description	Manager	System Status	System Phone	Minutes
Manager on page 257					
Viewing the card contents on page 248	View the folders and files on the control unit memory cards.	✓	–	–	–
The following procedures can be performed on cards in an SD card reader on a PC running Manager.					
Formatting an SD card on page 246	Reformat a card for B5800 Branch Gateway use without removing the Feature Key serial number. **Caution:** This process will erase all existing files on the card.	✓	✓	–	1
About creating a B5800 Branch Gateway SD card on page 246	Create the folder structure on a memory card and copy a set of B5800 Branch Gateway software files into those folders.	✓	–	–	15

Card specification

Non-Avaya cards can be used in the Optional SD card slot as long as they match or exceed the following standard:

SDHC 4GB minimum Class 2+. Single partition FAT32 format.

SD card folders

The System SD card contains the following folders:

- **primary** — contains the firmware files for the control unit, external expansion modules and supported phones. The folder can also contain music on hold files and license key files. This is the main set of files used by the B5800 Branch Gateway system when booting up. It also contains the stored copy of the B5800 Branch Gateway configuration.
- **backup** — contains a copy of the primary folder at some previous point. A backup copy of the primary contents to this folder can be invoked manually (using Manager or SSA) or as part of the B5800 Branch Gateway software upgrade using Manager.
- **lvmail** — a sub-folder that is used to store individual user and group mailbox messages, name recordings and announcements used by Embedded Voicemail. The storage capacity for Embedded Voicemail is limited to 15 hours regardless of the capacity of the card. Mailbox messages and greetings are stored in a sub-folder of the /dynamic folder.
- **AAG** — a sub-folder that is used to store embedded voicemail auto-attendant greetings.
- **doc** — contains initial installation documentation for B5800 Branch Gateway .

- **dynamic** — contains files used by the B5800 Branch Gateway and retained through a reboot of the B5800 Branch Gateway system.
- **temp** — contains temporary files used by the B5800 Branch Gateway and not retained through a reboot of the B5800 Branch Gateway system.

The Optional SD card can contain a similar set of folders as the System SD card. The Optional SD card folders are used as an additional backup or they can be used as the source for upgrading the contents of the System SD card.

Booting from the SD cards

When being powered up, the control unit looks for a valid .bin binary file to load. It does this using the possible source below in the order shown, skipping to the next source if the file is not present or is not valid.

1. System SD card primary folder.
2. The control unit's own internal non-volatile memory. Once a system has been installed, it uses its non-volatile memory to keep copies of the configuration and system binary files it is using. These can be used to restore operation during a system reboot. Note that though a system can boot from non-volatile memory, a System SD card must still be present for correct system operation.
3. System SD card backup folder.
4. Optional SD card primary folder.
5. Optional SD card backup folder.
6. If no file is found, the control unit will fallback to making BOOTP requests to the network. Manager can respond to the BOOTP request. See About erasing the operational firmware on page 235 for more information.

Once a valid .bin file is found, the control unit loads that firmware. The source from which the control unit binary file was loaded is then used to load further files.

Configuration file loading

After the system firmware files are installed, a configuration file must be installed on the control unit.

- If the control unit booted using binary files from an SD card location, it looks for a valid configuration file in the same location.
  - If a configuration file is present and valid, it is loaded.
  - If a configuration file is present but is not valid, load the configuration copy in its non-volatile memory if present. Otherwise, the control unit will have a default configuration.

- If a configuration file is not present, use the non-volatile memory copy unless the reboot is as a result of a default system command.

- If the control unit booted using binary files from its non-volatile memory, it will also load the configuration copy from that location.
  - It will indicate a boot alarm (see **Boot alarms** below).
  - It will attempt to restore the firmware file in the System SD card /primary folder using the copy in its non-volatile memory.
  - The normal boot-up process of upgrading expansion module firmware does not occur. If the **File** > **Advanced** > **Upgrade** command is used, only external expansion modules actually present in the system are listed for upgrade.

Post boot operation

During normal operation, configuration and binary files sent to the System SD card /primary folder using Manager are also written to the non-volatile memory.

If the system has booted from its non-volatile memory due to an SD card problem, it is still possible to upgrade the .bin file using the B5800 Branch Gateway upgrade wizard. See System upgrade using the System SD card on page 256 for more information.

Boot alarms

The following apply if the control unit boots up using software other than that in its System SD primary folder:

- An alarm will be shown in the System Status application. It will also generate an alarm if the card in any slot is not compatible. These alarms are also output as SNMP, Syslog or email alarms.
- The Manager **Select IP Office** window will display an ⚠

  icon indicating that the system is running using software other than from the System SD card's primary folder.
- The configuration can be read but will be read only. Attempting to send a configuration to the system will cause the error message `Failed to save configuration data. (Internal error)`.

Bypassing the System SD card primary folder

The control unit can be forced to bypass the System SD card's primary folder and non-volatile memory when starting. This is done by pressing the **AUX** button while applying power to the control unit. This may be necessary if, following an upgrade of the B5800 Branch Gateway system, it is determined that a roll back to the previously backed up firmware and configuration is required. Using the **AUX** button should restore system operation using the backup folder files while the installer then restores the contents of the primary folder to a previous release.

About creating a B5800 Branch Gateway SD card

The procedures in this section are for B5800 Branch Gateway SD cards for use in the System SD card slot. They can also be applied to non-Avaya SD cards for use in the Optional SD card slot. For the System SD card slot, only Avaya SD cards with a Feature Key should be used.

The card must be in the following format:

SDHC 4GB minimum Class 2+. Single partition FAT32 format.

⚠ Warning:

Avaya supplied SD cards should not be formatted using any other method than the format commands within Manager and the System Status application. Formatting the cards using any other method will remove the feature key used for B5800 Branch Gateway licensing from the card.

These procedures are run on an SD card inserted in a card reader on the Manager PC. That card can then be used in the System SD card slot of a new system or in the Optional SD card slot of an existing system to upgrade that system.

Formatting an SD card

Before you begin

To enable this option, the working directory defined in **File > Preferences > Directories** must be set to the parent directory of the Memory Cards folder.

About this task

Avaya SD cards should only be formatted using the format options provided within the B5800 Branch Gateway applications.

⚠ Warning:

This procedure will erase any existing files and folders on the card.

Procedure

1. Start Manager.
2. Insert the SD card into a reader slot on the Manager PC.
3. Select **File** > **Advanced** > **Format IP Office SD Card** > **Avaya B5800 Branch Gateway**.
4. Browse to the card location and click **OK**.

The status bar at the bottom of Manager displays the progress of the formatting process.

5. When the formatting is complete, load the B5800 Branch Gateway folders and files onto the card from the Manager PC. See Recreating an SD card on page 247.

Formatting a System SD card using the System Status application

Procedure

1. Start the System Status application and access the System Status output.
2. In the navigation panel, select **System > Memory Cards > System SD**.
3. Click on the **Format** button at the bottom of the screen.
   The card is reformatted. All files and folders on the card will be deleted. This process takes a few seconds.

Recreating an SD card

Before you begin

To enable this option, the working directory defined in **File > Preferences > Directories** must be set to the parent directory of the Memory Cards folder.

Be sure to back up the PLDSKeys.xml file in the primary folder before you perform this task. When you perform this task, the PLDSKeys.xml file is deleted.

About this task

This procedure creates the folder structure on the SD card and copies the required firmware files from those installed with Manager onto the SD card. This includes the binary files for the system, any external expansion modules, and phones. It also includes the prompt files for embedded voicemail operation.

This procedure can be used to upgrade an existing SD card to match the file set installed with Manager. For the card to be used in the System SD card slot, the card must be an Avaya SD Feature Key card. The card must be correctly formatted. See Formatting an SD card on page 246.

If the card contains any dynamic system files, for example SMDR records, they are temporarily backed up by Manager and then restored after the card is recreated. This procedure takes approximately 15 minutes.

Procedure

1. Insert the SD card into a card reader on the Manager PC.

Note:

Do not remove the SD card. Removing the SD card will interrupt the upgrade.

2. Select **File > Advanced > Recreate IP Office SD Card > Avaya B5800 Branch Gateway**.
3. Browse to the card location and click **OK**.
   Manager starts creating folders on the SD card and copying the required files into those folders. This process takes approximately 15 minutes. Do not remove the SD card until Manager shows a message that the recreation has finished.

Viewing the card contents

About this task

Using Manager you can view the folders and files on the System SD card and the Optional SD card.

Procedure

1. Start Manager.
2. Select **File > Embedded File Management**.
3. From the Select IP Office window, select the B5800 Branch Gateway system you want to view.
   The file contents of the memory cards are displayed.

About backing up the System SD card

There are two levels of backup that can be performed.

- **Backup the System SD card primary folder** — The contents of the primary folder on the System SD card are copied to the backup folder on the System SD. This can be performed remotely.
- **Backup all files on the System SD card** — The contents of the primary folder, backup folder, and embedded voicemail files including message files on the System SD card are copied to the Optional SD card. This can be performed remotely. However, the contents can only be copied back manually using a card reader.

Note:

The backup, restore, and copy operations will not be performed if the destination card has insufficient space for the files being copied.

Backing up the primary folder using Manager

About this task

This procedure copies the contents of the primary folder on the System SD card to the backup folder on the System SD card. Files with matching file names are replaced. This procedure takes approximately 6 minutes.

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File** > **Backup System Files**.
   The contents of the primary folder on the System SD card are copied to the backup folder. This process takes approximately 6 minutes.

Backing up the primary folder using the System Status application

Procedure

1. Start the System Status application and access the B5800 Branch Gateway status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Backup System Files**.
   The contents of the primary folder on the System SD card are copied to the backup folder. This process takes approximately 6 minutes.

Backing up the primary folder using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **System Backup**.
   The contents of the primary folder on the System SD card are copied to the backup folder. This process takes approximately 6 minutes.

About restoring from the backup folder

When you restore from the backup folder, you copy the contents of the backup folder on the System SD card to the primary folder on the System SD card. Files with matching file names are replaced.

⚠ Warning:

This procedure will cause the B5800 Branch Gateway system to be restarted, disconnecting any current calls and services in progress.

Restoring from the backup folder using Manager

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File** > **Restore System Files**.
   The contents of the backup folder on the System SD card are copied to the primary folder on the System SD card. The process takes approximately 6 minutes. When

the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring from the backup folder using the System Status application

Procedure

1. Start the System Status application and access the B5800 Branch Gateway status output.
2. In the navigation panel select **System**.
3. At the bottom of the screen select **Restore System Files**.
   The contents of the backup folder on the System SD card are copied to the primary folder on the System SD card. The process takes approximately 6 minutes. When the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring from the backup folder using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **System Restore**.
   The contents of the backup folder on the System SD card are copied to the primary folder on the System SD card. The process takes approximately 6 minutes. When the process has been completed, the B5800 Branch Gateway system is restarted.

About backing up to the Optional SD card

Backing up to the Optional SD card copies all files on the System SD card to the Optional SD card. This includes contents of the primary folder, backup folder, and embedded voicemail files including message files. Matching files and folders on the Optional SD card are overwritten.

Any files already copied that change while this process is running are not recopied. Any new files added (for example voicemail messages) while the process is running may not be copied.

Backing up to the Optional SD card takes at least 90 minutes and may take much longer depending on the amount of data to be copied. For example, it will take longer if embedded voicemail is being used by the B5800 Branch Gateway system to take messages.

Backing up to the Optional SD card using Manager

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File** > **Copy System Card**.
   The contents of the System SD card are copied to the Optional SD card. This takes at least 90 minutes and can take much longer.

Backing up to the Optional SD card using the System Status application

Procedure

1. Start the System Status application and access the B5800 Branch Gateway status output.
2. In the navigation panel select **System**.
3. Select **Memory Cards**.
4. Select **System Card**.

5. At the bottom of the screen select **Copy System Card**.
   The contents of the System SD card are copied to the Optional SD card. This takes at least 90 minutes and can take much longer.

Backing up to the Optional SD card using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **Copy**.
   The contents of the System SD card are copied to the Optional SD card. This takes at least 90 minutes and can take much longer.

About restoring from the Optional SD card

The files in the primary folder on the Optional SD card can be copied to the primary folder on the System SD card. Files with matching file names are replaced.

There are two levels of restore that can be performed:

- **Restoring only configuration files from the Optional SD card** — Only the configuration file config.cfg and the licenses file keys.txt are copied from the Optional SD card to the System SD card.
- **Restoring only software files from the Optional SD card** — All files in the primary folder *except* the configuration file config.cfg and licenses file keys.txt are coped from the Optional SD card to the System SD card. This process does not restore embedded voicmail prompts. This process takes approximately 5 minutes.

Being able to restore just the software files allows software files to be copied from an Optional SD card without affecting the existing configuration of that system.

⚠ Warning:

This procedure will cause the B5800 Branch Gateway system to be restarted, disconnecting any current calls and services in progress.

Restoring a configuration file from the Optional SD card using Manager

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File > Upgrade Configuration**.
   The configuration file config.cfg and licenses file keys.txt in the primary folder on the Optional SD card are copied to the primary folder on the System SD card. This takes a few seconds. When the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring a configuration file from the Optional SD card using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **Upgrade Config**.
   The configuration file config.cfg and licenses file keys.txt in the primary folder on the Optional SD card are copied to the primary folder on the System SD card. This

takes a few seconds. When the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring software files from the Optional SD card using Manager

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File > Upgrade Binaries**.
   All files in the primary folder on the Optional SC card except the configuration file config.cfg and licenses file keys.txt are copied to the primary folder on the System SD card. This takes approximately 5 minutes. When the process has been completed, the B5800 Branch Gateway system is restarted.

Restoring software files from the Optional SD card using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Select **Upgrade Binaries**.
   All files in the primary folder on the Optional SC card except the configuration file config.cfg and licenses file keys.txt are copied to the primary folder on the System SD card. This takes approximately 5 minutes. When the process has been completed, the B5800 Branch Gateway system is restarted.

System upgrade using the System SD card

In addition to using the upgrade wizard (see Using the upgrade wizard on page 217), control units can be upgraded by loading the required firmware files onto the System SD card and rebooting the system. There are several ways to load the required firmware onto the System SD card as described in the table below.

Note:

- Check the latest B5800 Branch Gateway Technical Bulletin for the B5800 Branch Gateway software release before proceeding any further. It may contain information relating to changes that occurred after this document was completed. Bulletins are available from http://support.avaya.com
- Some upgrades may require entry of upgrade licenses.

Warning:

This procedure will cause the system to be restarted, disconnecting any current calls and services in progress.

Method	Description	Location	Software Files	Embedded Voicemail Prompts
Upgrading remotely using Manager on page 257	Using Manager, the contents of the card are compared to the files that Manager has available and are upgraded if necessary.	**Local or Remote**	✓	✓
System SD Card Upgrade on page 257	In this method, the System SD card is shut down and removed from the control unit. The card's contents are upgraded using Manager.	**Local**	✓	✓
Upgrade from Optional SD Card on page 258	This method uses an SD card loaded with the required version of B5800 Branch Gateway software. The card is inserted into the control unit and then Manager, System Status or a system phone is used to transfer the software to the System SD card.	**Local**	✓	–

Upgrading remotely using Manager

About this task

This procedure copies all system files not present or of a different version compared to those already present on the System SD card.

Procedure

1. Start Manager.
2. Select **File** > **Embedded File Management**.
3. From the Select IP Office window, select the appropriate system.
   The file contents of the memory cards are displayed.
4. Select **File** > **Backup System Files**.
   The contents of the primary folder on the System SD card are copied to the backup folder. This process takes approximately 6 minutes.
5. Select **File** > **Upload System Files**.
   Manager uploads the system files to the primary folder on the System SD card. This includes B5800 Branch Gateway software files and embedded voicemail prompt files. Depending on the files that need to be updated, this can take up to40 minutes.

Upgrading the SD card locally

About this task

You can upgrade the SD card locally if you have physical access to the control unit. This method should be used with a timed reboot, allowing the card upgrade to be done during normal operation hours followed by a reboot outside of normal operation hours. See Rebooting the system on page 208 for more information.

If the card is being used for embedded voicemail, that service is not available while the card is shutdown. Licensed features however will continue running for up to 2 hours while the card is shutdown.

Procedure

1. Shutdown the System SD card and remove it from the control unit. See Memory card removal on page 259 for more information.
2. Create the SD card. See About creating a B5800 Branch Gateway SD card on page 246.

This procedure overwrites the software files on the card with the files available in Manager. It will not affect any other files, for example the configuration file. This process takes approximately 15 minutes.

3. Reinsert the card into the System SD card slot on the control unit.
4. Using Manager, select **File** > **Advanced** > **Reboot**.
5. In the Select IP Office window, select the appropriate system and click **OK**.
6. Select the type of reboot you want to perform and click **OK**.
   When the system reboots, the software files are loaded in the primary folder of the System SD card.

Upgrading using an Optional SD card

About this task

This method allows an Optional SD card to be used as the source from which the System SD card is upgraded. It only upgrades the software files, it does not update embedded voicemail prompts.

Procedure

1. Insert the SD card into a card reader on the Manager PC.

   Note:

   Do not remove the SD card. Removing the SD card will interrupt the upgrade.
2. Using Manager, select **File** > **Advanced** > **Recreate IP Office SD Card**.
3. Select one of the following:

   - **IP Office A-Law**
   - **IP Office U-Law**

   This selection determines how the system operates when defaulted with the SD card installed in the System SD card slot.
4. Browse to the card location and click **OK**.
   Manager starts creating folders on the SD card and copying the required files into those folders. This process takes approximately 15 minutes. Do not remove the SD card until Manager shows a message that the recreation has finished.
5. Insert the card into the Optional SD card slot on the control unit.
6. Use one of the following procedures to copy the software from the Optional SD card to the System SD card:

   - See Restoring software files from the Optional SD card using Manager on page 255.

- See Restoring software files from the Optional SD card using a system phone on page 255.

Memory card removal

Warning:

Memory cards should always be shut down before being removed when the system is running. Though the card slot LEDs indicate when data is being written to a card, lack of flashing LEDs is not a sufficient safeguard. Shutting down the card will disable embedded voicemail if being used. If the System SD card is removed, features licensed by the card's Feature Key serial number will continue operating for up to 2 hours.

Card services can be restarted by either reinserting the card or using a Start Up command.

Shutting down a memory card using Manager

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. Select **File** > **Advanced** > **Memory Card Command** > **Shutdown**.
   The following prompt appears: **Shutting down a memory card may cause service loss. Continue?**
3. Click **Yes**.
4. In the Select IP Office window, click the check box for the appropriate system.
5. Click **OK**.
6. At the back of the control unit, confirm that the appropriate memory card LED is off.
7. Remove the card.

Shutting down a memory card using a system phone

About this task

To shut down a memory card using a system phone, you must be administered as a System Phone user. You can shut down a memory card using a 1400, 1600, or 9600 series phone. Your Login Code is used to restrict access to some system administration functions on the phone.

Procedure

1. Select **Features > Phone User > System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. Select **Memory Card**.
4. Select **System** for the System SD card or **Option** for the Optional SD card.
5. Select **Shutdown**.
6. At the back of the control unit, confirm that the appropriate memory card LED is off.
7. Remove the card.

Shutting down a memory card using System Status

Procedure

1. Open System Status and access the status output.
2. In the navigation pane, select **System > Memory Cards**.
3. Click **System SD** or **Optional SD**.
4. At the bottom of the window, click **Shutdown**.
5. At the back of the control unit, confirm that the appropriate memory card LED is off.
6. Remove the card.

Memory card startup

Reinserting a memory card into a system that is already switched on will automatically restart card operation. However, if the card has been shutdown but not removed, it can be restarted without requiring a reboot.

Starting up a memory card using Manager

About this task

Use this task to restart a memory card without removing and reinserting it.

Perform this task using IP Office Manager that is installed on a PC for the branch. You cannot perform this task from Manager that is accessed from System Manager. If the B5800 Branch Gateway is centrally managed by System Manager, you must disable the System Manager administration feature for the branch (by disabling **Under SMGR Administration** in Security Settings) before you perform this task. For more information, see “Disabling the System Manager administration feature for the branch” in *Implementing the B5800 Branch Gateway for an Avaya Aura® Configuration*, document number 18-603853.

Procedure

1. Open IP Office Manager and receive the B5800 Branch Gateway configuration.
2. Select **File > Advanced > Memory Card Command > Startup**.
3. In the Select IP Office window, click the check box for the appropriate system.
4. Click **OK**.

Starting up a memory card using System Status

About this task

Use this task to restart a memory card without removing and reinserting it.

Procedure

1. Open System Status and access the status output.
2. In the navigation pane, select **System > Memory Cards**.
3. Click **System SD** or **Optional SD**.

4. At the bottom of the window, click **Startup**.

Starting up a card using a system phone

About this task

A user configured as a system phone user can perform this procedure using a 1400, 1600, or 9600 Series phone (excluding XX01, XX02 and XX03 models). The user's login code is used to restrict access to system administration functions on the phone.

Procedure

1. Select **Features** > **Phone User** > **System Admin**.
2. Enter your B5800 Branch Gateway user login code.
3. From the menu select **Memory Card**.
4. Choose one of the following:
   - Select **System** for the System SD card
   - Select **Option** for the Optional SD card.
5. Select **Startup**.

Chapter 17: Safety and regulatory information

Safety statements

The B5800 Branch Gateway modules are intended to be installed by Service Personnel and it is the responsibility of the Service Personnel to ensure that all subsidiary interconnected equipment is wired correctly and also meet the safety requirements of IEC60950 or UL60950 where applicable.

- CE
  The CE mark affixed to this equipment means that the module complies with the 1999/5/EC (R&TTE), 89/336/EEC (EMC) and 72/23EEC (LVD) Directives.
- The Declarations of Conformity (DoC) for the B5800 Branch Gateway products are available on the B5800 Branch Gateway Application DVD.
- **⚠ Warning:**
  This warning symbol is found on the base of B5800 Branch Gateway modules.
- Refer to Trunk Interface Modules on page 265 for information concerning which trunk interface module variants are fitted in which country.

In Finland, Norway and Sweden a protective earthing conductor must be attached to the protective earth point on the rear of the servers. See Grounding on page 71 for more information. In addition, the server must be located in a restricted access location where equipotential bonding has been applied, for example, in a telecommunication center.

Important safety instructions when using your telephone equipment

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord and batteries indicated in this manual.

Lithium batteries

A lithium battery is fitted to the real time clock on the control unit motherboard.

⚠ Warning:

The Lithium battery must only be replaced by Avaya personnel or authorized representatives. There is a danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Lightening protection/hazard symbols

Lightning protectors — The buildings lightning protectors must be verified as follow:

1. Check the lightning protectors at the trunk cable entry point to the building housing the B5800 Branch Gateway system , paying special attention to the lightning protection grounding. Report any problems, in writing, to the telephone company.
2. Equipment that is designed to be connected using internal wiring is typically not lightning protected. Hence, B5800 Branch Gateway extension cabling must not leave the building. For installations where telephones and/or other standard (tip/ring) devices are installed in another building then lightning protection is required, see Out of Building Telephone Installations on page 72.

Hazard Symbol — The shock hazard symbol is intended to alert personnel to electrical hazard or equipment damage. The following precautions must also be observed when installing telephone equipment:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Always use caution when working with telephone lines.

Trunk interface modules

To ensure the validation of the approvals, only the following types of trunk interface cards must be fitted in the B5800 Branch Gateway control unit.

USA/Canada							
Product	**Quad BRI**	**PRI E1**		**PRI T1**		**ATM4**	**WAN**
		Single	**Dual**	**Single**	**Dual**		
Control unit	✗	✗	✗	✓	✓	✓	✗

Rest of World							
Product	**Quad BRI**	**PRI E1/E1R2**		**PRI T1**		**ATM4**	**WAN**
		Single	**Dual**	**Single**	**Dual**		
Control unit	✓	✓	✓	✗	✗	✓	✗

Note:

E1R2 trunks are only supported in CALA and Korea.

Port safety classification

The B5800 Branch Gateway systems have the following ports which are classified as follows:

Port Name	Port Description	Port Classification
PRI port	PRI ISDN connection (NET)	TNV (Operating within the limits of SELV)
BRI ports	BRI ISDN connection (NET)	TNV (Operating within the limits of SELV)
Analog ports	Two wire analog trunk	TNV3
Power fail ports	Two wire analog trunk	TNV3
DTE port	Async Data connection.	SELV
Analog telephone ports	Telephone Extension ports	TNV2
Digital telephone ports	Telephone Extension ports	SELV
WAN port	WAN connection (NET).	SELV
LAN ports	10/100 BaseT attachment to LAN.	SELV

Port Name	Port Description	Port Classification
Expansion ports	Expansion Module connector.	SELV
Audio port	Connector for Music on Hold.	SELV
External control port	Connector for Controlling Ancillary circuits.	SELV
DC input port	Connector for DC input power.	SELV

Interconnection circuits shall be selected to provide continued conformance with the requirements of EN 609050:1992/A3:1995 clause 2.3 for SELV circuits and with the requirements of clause 6 for TNV circuits, after connections between equipment.

EMC cautions

889/336/ EEC (EMC Directive) CISPR 22:1993 including A1 + A2, AS/NZ 3548:1995 (ROW)

⚠ Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

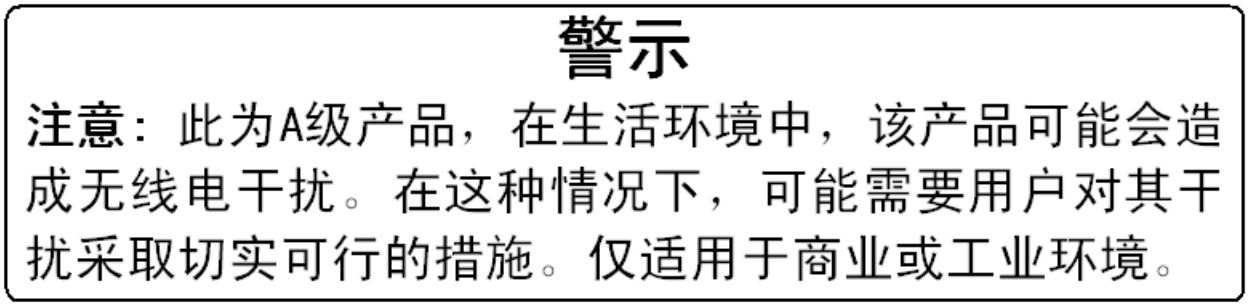
Federal communications commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.

Canadian department of communications (DOC)

"NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment."

EMC caution for china



Regulatory Instructions for Use

Australia

BRI interface

During the configuration, ensure "000" emergency number is not barred, by performing the following:

- Short Code: 000
- Telephone No: 000;
- Function: DialEmergency

Connections to TS013, the following bearer capabilities shall not be used: 7kHz Audio, Video, Restricted Digital Information.

If unknown type of number is used in calling party number, the network will use the default CLI.

The system must be configured for Point to Multi point connection to comply with Austel requirements for connecting to TS013 circuits.

As the B5800 Branch Gateway does not support emergency dialing after loss of power, the following warning notice should be recognized:

⚠ Warning:

This equipment will be inoperable when main power fails.

PRI interface

During the configuration, ensure "000" emergency number is not barred, by performing the following:

- Short Code: 000
- Telephone No: 000;
- Function: DialEmergency

Canada

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met.

It does not imply that Industry Canada approved the equipment.

"NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is 1. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five."

China

AVAYA

700433220
February 2007
Copyright© 2007, Avaya Inc. All Rights Reserved

所有在中华人民共和国境内进口或销售的电子信息产品必须附上本文件

Include this document with all Electronic Information Products imported or sold in the People's Republic of China

部件名称 (Part Name)	有毒有害物质或元素 (Hazardous Substance)					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件 (Metal Parts)	×	○	○	○	○	○
电路模块 (Circuit Modules)	×	○	○	○	○	○
电缆及电缆组件 (Cables & Cable Assemblies)	×	○	○	○	○	○
塑料和聚合物部件 (Plastic and Polymeric parts)	○	○	○	○	○	○
电路开关/断路器 (Circuit Switch/Breakers)	○	○	○	○	○	○
电源组件 (Power Assemblies)	×	○	○	○	○	○
显示器 (LCD, Monitor)	○	○	○	○	○	○
玻璃 (Glass)	○	○	○	○	○	○

○： 表示该有毒有害物质在该部件所有均质材料中的含量均在 SJ/T 11363 2006 标准规定的限量要求以下。
Indicates that the concentration of the hazardous substance in all homogeneous materials in the parts is below the relevant threshold of the SJ/T 11363 2006 standard.

×： 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363 2006 标准规定的限量要求。
Indicates that the concentration of the hazardous substance of at least one of all homogeneous materials in the parts is above the relevant threshold of the SJ/T 11363 2006 standard.

本表显示，所附的亚美亚电子信息产品中，从生产日期起，可能包含这些物质。注意：所附产品可能包含或不含以上所列的某些组件。
This table shows where these substances may be found in Avaya's electronic information products, as of the date of manufacture of the enclosed product. Note that some of the component types listed above may or may not be a part of the enclosed product.

除非有另外特别的标注,此标志将作为所附产品及零部件的环保使用期标志. 某些产品会有一个不同的环保使用期(例如,电话机)并贴在其产品上.此环保使用期限只适用于产品在产品手册中所规定的条件下使用

The Environmentally Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain products have a different EFUP (for example, telephones) and so are marked to reflect such. The Environmentally Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

European Union

- 999 and 112 calls must not be barred. Doing so will invalidate the approval.
- All connections at the MDF shall be identifiable by suitable labeling.
- The CE mark displayed on B5800 Branch Gateway equipment indicates the systems compliance with the EMC, LVD, and R&TTE Directives and common technical regulations for Primary Rate and Basic Rate ISDN.
- All ports for the connection of other non-telecommunications apparatus have a Safety Extra Low Voltage (SELV) safety status.

New Zealand

The grant of a Telepermit for any item of terminal equipment indicates only that Telecom has accepted that the item complies with minimum conditions for connection to its network. It indicates no endorsement of the product by Telecom, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of Telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Telecom's network services.

FCC notification

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of connection

Connection of this equipment to the telephone network is shown in the following table.

Port	FIC	SOC	USOC Jack	REN
IPO500 PRI 1U, IPO500 PRI2U, IP400 PRI-T1	04DU9.BN, 04DU9.DN, 04DU9.IKN, 04DU9.ISN	6.0Y	RJ48C	NA
IPO500 ATM4U IP400 ATM4U	OL13A, OL13B, OL13C, 02AC2, 02LA2, 02LB2, 02LC2, 02LR2, 02LS2	9.0Y	RJ45S	0.1B
IPO500 ATM16	OL13A, OL13B, OL13C, 02AC2, 02GS2, 02LA2, 02LB2, 02LC2, 02LR2, 02LF2 02GS2, 02LS2	9.0Y	RJ45S	0.1B

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Equipment with Direct Inward Dialing (DID)

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC’s rules.

Proper answer supervision is when:

- This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
  - Answered by the called station
  - Answered by the attendant

- Routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
- Routed to a dial prompt

• This equipment returns answer supervision signals on all DID calls forwarded back to the PSTN. Permissible exceptions are:

- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic dialers

When programming emergency numbers and (or) making test calls to emergency numbers:

• Remain on the line and briefly explain to the dispatcher the reason for the call.

• Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll restriction and least cost routing equipment

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer’s employees from gaining access to the network and to these codes.

FCC part 68 supplier’s declarations of conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC’s Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Compliance with FCC rules

Transmit and receive gain settings for PRI/T1 and analog ports

The Gain settings are password controlled for use by qualified installation personnel only and must not be made available to the end user. The default gain settings of 0dB ensures compliance with FCC part 68 section 68.308(b)(5) and TIA/EIA-IS-968 Section 4.5.2.5. "Through transmission amplification from ports for the connection of separately registered equipment or from other network connection ports". Gain setting adjustment by unqualified

personnel may result in violation of the FCC rules. Qualified personnel may adjust gain settings above these levels only where:

- Measurement is made to ensure that the power levels sent to line at each network interface connected does not exceed the maximum levels specified in FCC part 68 section 68.308(b) and TIA/EIA-IS-968 Section 4.5 for that specific interface type.
- Where gain adjustment away from the default values are made, precautions should be taken to ensure that the connection of terminal equipment is controlled by qualified installation personnel.
- To conform with the Receive Objective Loudness Rating at distances greater than 2.7km from the central office, on analog trunks a receive gain of 1.5dB must be set.

Appendix A: Avaya port matrix for B5800 Branch Gateway and SIP phones

This appendix provides example ingress and egress ports for B5800 Branch Gateway and SIP phones.

What are ports and how are they used?

TCP and UDP use ports (defined at http://www.iana.org/assignments/port-numbers) to route traffic arriving at a particular IP device to the correct upper layer application. These ports are logical descriptors (numbers) that help devices multiplex and de-multiplex information streams. Consider your desktop PC. Multiple applications may be simultaneously receiving information. In this example, email may use destination TCP port 25, a browser may use destination TCP port 80 and a telnet session may use destination TCP port 23. These logical ports allow the PC to de-multiplex a single incoming serial data packet stream into three mini-streams inside the PC. Furthermore, each of the mini-streams is directed to the correct high-level application because the port numbers identify which application each data mini-stream belongs. Every IP device has incoming (Ingress) and outgoing (Egress) data streams.

Ports are used in TCP and UDP to name the ends of logical connections which carry data flows. TCP and UDP streams have an IP address and port number for both source and destination IP devices. The pairing of an IP address and a port number is called a socket (discussed later). Therefore, each data stream is uniquely identified with two sockets. Source and destination sockets must be known by the source before a data stream can be sent to the destination. Some destination ports are “open” to receive data streams and are called “listening” ports. Listening ports actively wait for a source (client) to make contact to a destination (server) using a specific port that has a known protocol associate with that port number. HTTPS, as an example, is assigned port number 443. When a destination IP device is contacted by a source device using port 443, the destination uses the HTTPS protocol for that data stream conversation.

Port type ranges

Port numbers are divided into the following three ranges:

- Well known ports are those numbered from 0 through 1023.
- Registered ports are those numbered from 1024 through 49151
- Dynamic ports are those numbered from 49152 through 65535

The well known and registered ports are assigned by IANA (Internet Assigned Numbers Authority) and are found at http://www.iana.org/assignments/port-numbers.

Well known ports

For the purpose of providing services to unknown clients, a service listen port is defined. This port is used by the server process as its listen port. Common services often use listen ports in the well known port range. A well known port is normally active meaning that it is “listening” for any traffic destined for a specific application. For example, well known port 23 on a server is actively waiting for a data source to contact the server IP address using this port number to establish a Telnet session. Well known port 25 is waiting for an email session, etc. These ports are tied to a well understood application and range from 0 to 1023.

In UNIX and Linux operating systems, only root may open or close a well known port. Well known ports are also commonly referred to as privileged ports.

Registered ports

Unlike well known ports, these ports are not restricted to the root user. Less common services register ports in this range. Avaya uses ports in this range for call control. Some, but not all, ports used by Avaya in this range include: 1719/1720 for H.323, 5060/5061 for SIP, 2944 for H.248 and others. The registered port range is 1024 – 49151. Even though a port is registered with an application name, industry often uses these ports for different applications. Conflicts can occur in an enterprise when a port with one meaning is used by two servers with different meanings.

Dynamic ports

Dynamic ports, sometimes called private ports, are available to use for any general purpose. This means there are no meanings associated with these ports (similar to RFC 1918 IP Address Usage). These are the safest ports to use because no application types are linked to these ports. The dynamic port range is 49152 – 65535.

Sockets

A socket is the pairing of an IP address with a port number. An example would be 192.168.5.17:3009, where 3009 is the socket number associated with the IP address. A data flow, or conversation, requires two sockets – one at the source device and one at the destination device. The data flow then has two sockets with a total of four logical elements. Each data flow must be unique. If one of the four elements is unique, the data flow is unique. The following three data flows are uniquely identified by socket number and/or IP address.

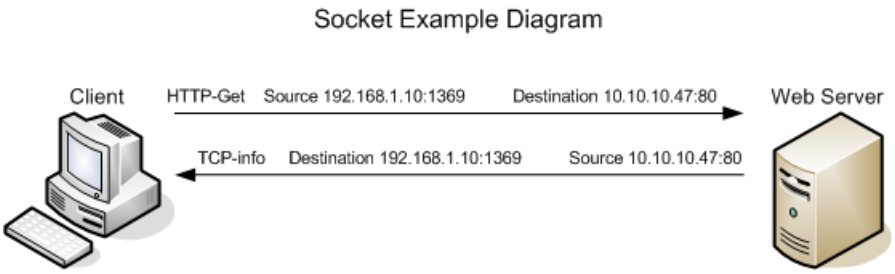
- Date flow 1: 172.16.16.14:1234 — 10.1.2.3:2345
- Date flow 2: 172.16.16.14:1235 — 10.1.2.3:2345
- Date flow 3: 172.16.16.14:1234 — 10.1.2.4:2345

Data flow 1 has two different port numbers and two different IP addresses and is a valid and typical socket pair.

Data flow 2 has the same IP addresses and the same port number on the second IP address as data flow 1, but since the port number on the first socket differs, the data flow is unique.

Therefore, if one IP address octet changes, or one port number changes, the data flow is unique.

Socket example showing ingress and egress data flows from a PC to a web server



Notice the client egress stream includes the client's source IP and socket (1369) and the destination IP and socket (80). The ingress stream has the source and destination information reversed because the ingress is coming from the server.

Firewall types

There are three basic firewall types described below.

Packet filtering

Packet Filtering is the most basic form of the firewalls. Each packet that arrives or leaves the network has its header fields examined against criterion to either drop the packet or let it through. Routers configured with Access Control Lists (ACL) use packet filtering. An example of packet filtering is preventing any source device on the Engineering subnet to telnet into any device in the Accounting subnet.

Application level gateways

Application level gateways (ALG) act as a proxy, preventing a direct connection between the foreign device and the internal destination device. ALGs filter each individual packet rather than blindly copying bytes. ALGs can also send alerts via email, alarms or other methods and keep log files to track significant events.

Hybrid

Hybrid firewalls are dynamic systems, tracking each connection traversing all interfaces of the firewall and making sure they are valid. In addition to looking at headers, the content of the

packet, up through the application layer, is examined. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Stateful inspection firewalls close off ports until the connection to the specific port is requested. This is an enhancement to security against port scanning. Port scanning is the act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

Firewall policies

The goals of firewall policies are to monitor, authorize and log data flows and events. They also restrict access using IP addresses, port numbers and application types and sub-types. This appendix focuses on identifying the port numbers used by Avaya products so effective firewall policies can be created without disrupting business communications or opening unnecessary access into the network.

Knowing that the source column in the port usage tables provided below is the socket initiator is key in building some types of firewall policies. Some firewalls can be configured to automatically create a return path through the firewall if the initiating source is allowed through. This option removes the need to enter two firewall rules, one for each stream direction, but can also raise security concerns.

Another feature of some firewalls is to create an umbrella policy that allows access for many independent data flows using a common higher layer attribute. Finally, many firewall policies can be avoided by placing endpoints and the servers that serve those endpoints in the same firewall zone.

TFTP port usage

IP Office upgrade wizard and VM Pro all use TFTP for commands and data transfer. B5800 Branch Gateway implements a version of the TFTP Transfer Identifier mechanism (TID) defined by RFC 1350.

The general mechanism is each has a TFTP listener on port 69, any received command (READ request) is responded to with a TFTP response (WRITE request) to port 69. Any subsequent data transfer uses the source ports from both request and response.

IP Office Manager (upgrade wizard)	B5800 Branch Gateway
TFTP Read, src port 2421, dst port 69 >	
	< TFTP Write, src port 4153, dst port 69

	< TFTP Data packet (1..n), src port 4153, dst port 2421
TFTP Acks (1..n), src port 2421, dst port 4153	

Ingress ports for B5800 Branch Gateway and SIP phones

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
1	22	TCP/ SSH	No	Open	Admin terminal or SAL Gateway	Yes	System mgmt requiring shell access – Remote maintenance.
2	69	UDP/ TFTP	No	Open	NM/ Manager	Yes	B5800 Branch Gateway status, configuration data, program data. See Port type ranges on page 275 for ranges.
3	80	TCP/ HTTP	No	Open	NM/ Manager	Yes	Web client access, Inter B5800 Directory Exchange (optional).
4	123	UDP/ NTP	No	Open	NTP Server	Yes	NTP (RFC4330) Service.
5	161-C	UDP/ SNMP	Yes	Closed	Admin terminal or NMS	Yes	Read-only access to MIB entries.
6	5060	TCP/SIP	No	Open		Yes	SIP Signaling.
7	49152 – 53247-C	UDP/ RTP-RTCP	Yes	Open	IP Phones, RTCP Collector	Yes	Dynamically allocated ports used during VoIP calls for RTP and RTCP traffic. The port range can be adjusted through the System > Gatekeeper tab.
8	50802	TCP/ Who Is?	Yes	Open	B5800 Manager	Yes	TCP Discovery.

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
9	50805-C	TCP/ HTTP B5800 config access	No	Open	B5800 Manager	Yes	B5800 Configuration Service – Secured. See optional 50804.
10	50808-C	TCP/ HTTP B5800 Sys Status Access	No	Open	B5800 Manager	Yes	B5800 System Status Access.
11	50813-C	TCP/ HTTP B5800 Sec Settings Access	No	Open	B5800 Manager	Yes	B5800 Security Settings Access – Secured. See optional 50812.
OPTIONAL							
I-A	68	UDP/ DHCP-Cli	Yes	Open	DHCP-Srv	Yes	If configured, B5800 obtains its' IP address from a remote server.
I-B	443	TCP/ HTTP	No	Open	Dect R4	Yes	File transfer Web client access.
I-C	1718	TCP/ H323-Disc	No	Open	Branch Trunk	No	Offering H.323 service to IP phones.
I-D	1719	TCP/ RAS	No	Open	IP Phones	No	Offering H.323 service to IP phones.
I-E	5061	TCP/ TLS	Yes	Closed	Session Manager	Yes	Encrypted SIP signaling.
I-F	50796	UDP/ Partner App	Yes	Closed	Phone Mgr	Yes	Control of telephones from Phone Manager, Soft Console.
I-G	50804-C	TCP/ HTTPS B5800 Config Access	No	Open	B5800 Manager	Yes	B5800 Configuration Service – Unsecured. See 50805.
I-H	50812-C	TCP/ HTTP	No	Open	B5800 Manager	Yes	B5800 Security Settings Access –

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
		B5800 Sec Settings Access					Unsecured. See 50813.

For a description of the column headings, see Table column heading definitions on page 283.

Egress ports for B5800 Branch Gateway and SIP phones

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
1	53	UDP/ DNS	No	Open	DNS Server	Yes	DNS service to resolve URL and IP addresses.
2	69	UDP/ TFTP	No	Open	Manager	Yes	B5800 Branch Gateway status, configuration data, program data. See Port type ranges on page 275 for ranges.
3	123	UDP/ NTP	No	Open	NTP Server	Yes	NTP (RFC4330) Service.
4	162	UDP/ SNMP	Yes	Closed	Trap Receiver	Yes	Trap generation from B5800 Branch Gateway.
5	389	TCP/ LDAP	Yes	Closed	LDAP Server	Yes	Import of directory information from LDAP database.
6	500	UDP/ IKE	Yes	Closed	Security device	Yes	Form IPSec associations with remote security devices. Requires license.

#	Dest. Port	Network /App Protocol	En or Dis ?	Default Port State	Remote Device	Ext to Branch ?	Description
7	514	UDP/ Syslog-Cli	Yes	Open	Syslog Server	No, but could be	Log files transmitted from IP phones to server.
8	5005-C	RTCP	Yes	Open	NMS	Yes	RTCP collector (HP-Openview, AIM, etc.).
9	5060	TCP/SIP	No	Open		Yes	SIP signaling.
10	49152 – 53247-C	UDP/ RTP-RTCP	Yes	Open	IP Phones, RTCP Collector	Yes	Dynamically allocated ports used during VoIP calls for RTP and RTCP traffic. The port range can be adjusted through the System > Gatekeeper tab.
11	50794	UDP/ TCP/ Monitor	No	Open	Manager	Yes	Event, trace and diagnostic outputs.
OPTIONAL							
E-1	25	TCP/ SMTP	Yes	Open	Mail Server	Depends	
E-2	37	UDP/ Time	Yes	Closed	Manager	Yes	TIME (RFC868) Service supported by Manager and VMPro. Requested by B5800 Branch Gateway. This service is an option to NTP – port 123.
E-3	67	UDP/ DHCP-Srv	Yes		IP Clients	No	DHCP service to IP phones, PCs and other clients.
E-4	1720	TCP/ H323	Yes	Open	H323 Server	No	Offering H.323 service to IP phones.
E-5	5061	TCP/ TLS	Yes	Closed	Session Manager	Yes	Encrypted SIP signaling.

For a description of the column headings, see Table column heading definitions on page 283.

Table column heading definitions

Column heading	Description
Dest Port	Destination port — this is the layer-4 port number to which the connection request is sent. Valid values include 0 – 65535.
Network/App Protocol	Network/application protocol — this is the name associated with the layer-4 protocol and layers-5-7 application.
En or Dis?	Optionally Enabled or Disabled? — this field indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid values are Yes or No. • No means the default port state cannot be changed (that is, enable or disabled). • Yes means the default port state can be changed (that is, enabled or disabled).
Default Port State	Default Port State — a port is either open, closed, filtered or N/A. • Open ports will respond to queries. • Closed ports may or may not respond to queries and are only listed when they can be optionally enabled. • Filtered ports can be open or closed. Filtered UDP ports will not respond to queries. Filtered TCP will respond to queries, but will not allow connectivity. • N/A is used for the egress default port state since these are not listening ports on the product.
Remote Device	Remote Device — this is the remote device that is initiating a connection request (Ingress Connections) or receiving a connection request (Egress Connections).
Ext to Branch?	External to Branch? — this indicates whether traffic to this layer-4 port is needed between the branch and other sites, requiring this port to be open on firewalls, if any, between the branch and the rest of the customer's network. Note that this depends on the customer's deployment. Valid Values are: • Yes (meaning typically needed) • No (meaning not expected to be needed) • Depends (on customer deployment)

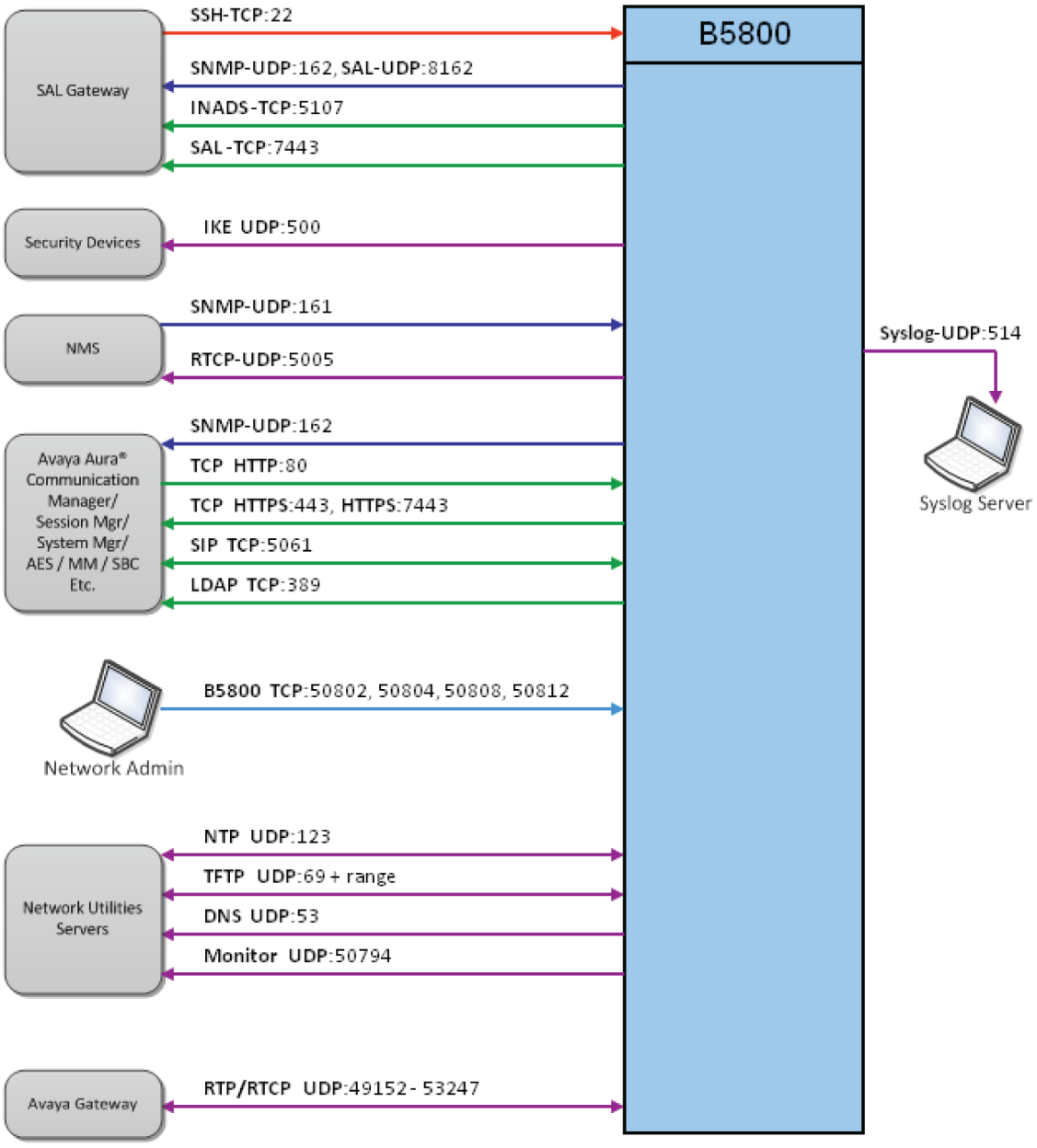
Notes:

- Email will not flow through the B5800 Branch Gateway in this example. See optional section for port 25.
- An off-site DHCP server is used to supply IP addresses to phones and PCs. Otherwise, add ports 67 and 68 in optional sections.
- The B5800 Branch Gateway IP address will be manually configured and not need a DHCP server.
- TFTP service begins using port 69, but eventually uses the source ports from both sides.
- Ports 80804 and 80812 are unsecure communications but have optional port 80805 and 80813 as secure options.
- For B5800 Branch Gateway R6.1, the TFTP/UDP port selection is an issue; IP Office Manager, ENM, and SysMonitor do not constrain the selection of TFTP/UDP source port.

  B5800 Branch Gateway R6.2 improves this TFTP port issue greatly in a number of ways:

  - System Manager does not use TFTP.
  - SysMonitor and IP Office Manager have configurable TFTP/UDP port ranges.
- HTTPS is used for DECT R4 administration.

Port usage diagram



In this diagram, direction of the arrow depicts call initiation. Data traffic will typically be 2-way.

Appendix B: B5800 Branch Gateway call flows

Calls from local extensions (i.e. deployed in the distributed branch user model)

1. Local phone to local phone

   Local phone A → B5800 Branch Gateway → local phone B

2. Local phone to PSTN (using local trunking)

   Local phone → B5800 Branch Gateway → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP Trunk) → PSTN

3. Local phone to PSTN (using centralized trunking)

   Local phone → B5800 Branch Gateway → Session Manager→ central gateway/SBC → PSTN

4. Local phone to headquarters or other enterprise site

   Local phone → B5800 Branch Gateway → Session Manager → target phone's controller → target phone

Calls to local extensions (i.e. deployed in distributed branch user model)

1. From PSTN to local extension via IP Office auto-attendant (branch auto-attendant LDN is associated with local B5800 Branch Gateway trunk)

   PSTN → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP trunk) → B5800 Branch Gateway auto-attendant → caller enters extension number → local phone

2. From PSTN direct to Local phone's DID (LDN is associated with local B5800 Branch Gateway trunk)

   PSTN → B5800 Branch Gateway trunk (e.g. FXO, ISDN, SP SIP trunk) → B5800 Branch Gateway → local phone

3. From headquarters (or other enterprise site) to local phone's enterprise number

   Originating phone → originating phone's controller → Session Manager → B5800 Branch Gateway → local phone

4. From headquarters (or other enterprise site) to local extension via IP Office auto-attendant

   Originating phone → originating phone's controller → Session Manager → B5800 Branch Gateway → B5800 Branch Gateway auto-attendant → caller enters extension number → local phone

Appendix C: Branch PSTN call routing examples

Each B5800 Branch Gateway system can support its own external PSTN trunks. When deployed in an Avaya Aura® network, you have considerable flexibility over where outgoing PSTN calls should emerge from the network and similarly where incoming calls should be routed.

The following examples demonstrate some of the options available:

- Centralized call control on page 289 — External calls at a branch site can be rerouted to be dialed out at another site. This can be done for reasons of call cost and call control. For example, the central site may have a bulk call tariff for national and international calls that would benefit all branches.
- Branch PSTN Override on page 292 — Having configured the branch to send outgoing external calls to the Avaya Aura® Session Manager for onward routing, there may be cases where a specific number should still be routed via the branches own PSTN trunks.
- PSTN Fallback on page 294 — The B5800 Branch Gateway can be configured to allow some calls that would normally use the Avaya Aura® Session Manager line to be routed via the PSTN when the Avaya Aura® Session Manager line is not available.

The various methods used in these examples can be combined to match the customer's needs. However the main aim should be as follows:

- To keep the branch configuration as generic as possible, i.e. to use the same PSTN call control in all branch configurations. This simplifies maintenance of multiple branches.
- To centralize as much of the PSTN call control in the Avaya Aura® Session Manager as possible. Again this simplifies maintenance and control.

Centralized call control

External calls at a branch site can be rerouted to be dialed out at another site, typically the headquarters site. This can be done for reasons of call cost and control and to reduce the external PSTN capacity required at the individual branch sites.

For example, we can route all national and international calls to the headquarters site to benefit from a bulk cost reduction available for calls from that site. The Avaya Aura® Session Manager there routes the calls out via PSTN services at that site. Note, however, that the Avaya Aura® Session Manager could alternately use the trunks at a branch for some calls. For example, if the national call is to an area code that is local to a particular branch, the call could be routed to that branch for dialing on its PSTN trunks.

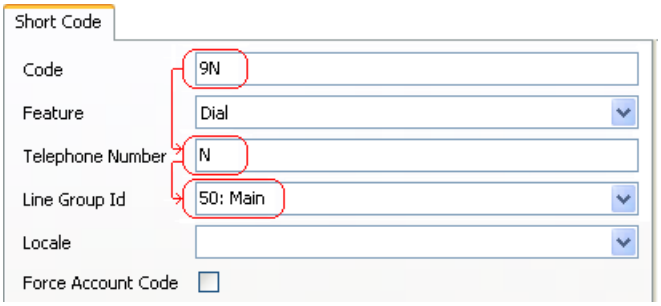
Routing B5800 Branch Gateway calls — example

About this task

This example assumes that all the branches were initially setup with the default North American locale. For B5800 Branch Gateway that means that a dial 9 prefix is used for external calls. For calls in other locales or between branches in different locals, the example would be adjusted to ensure that the resulting number received at the remote branch would be routed to an external PSTN trunk and is suitable for external dialing.

At each B5800 Branch Gateway, we need to ensure that calls starting with 90, the external and then international number prefixes, are routed to the branch's Avaya Aura® Session Manager line rather than direct to an external PSTN line.

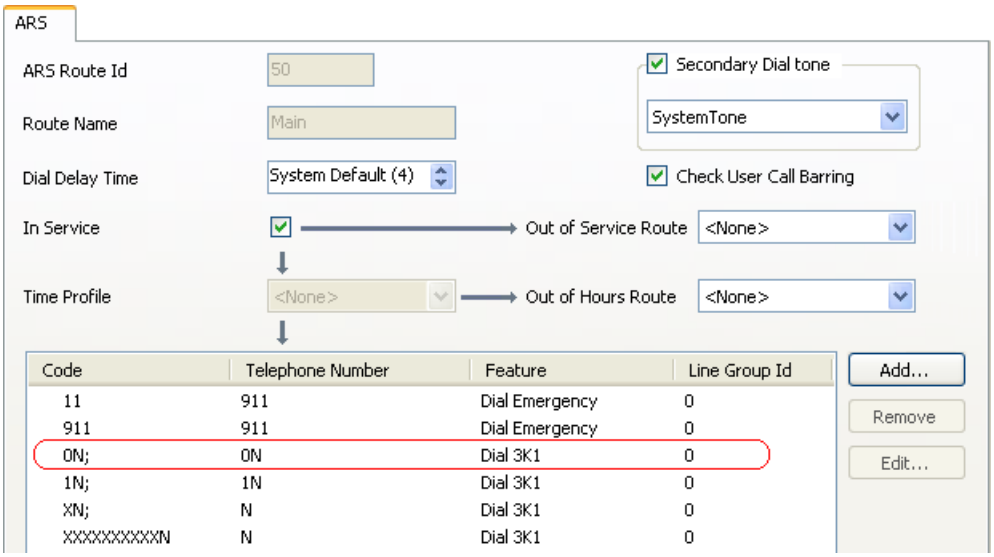
In the B5800 Branch Gateway system configuration, the default system short code **9N** is used to match calls prefixed with a 9. The short code removes the 9 prefix and routes the call to the branch's ARS form **50: Main**.



Procedure

1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **ARS**.

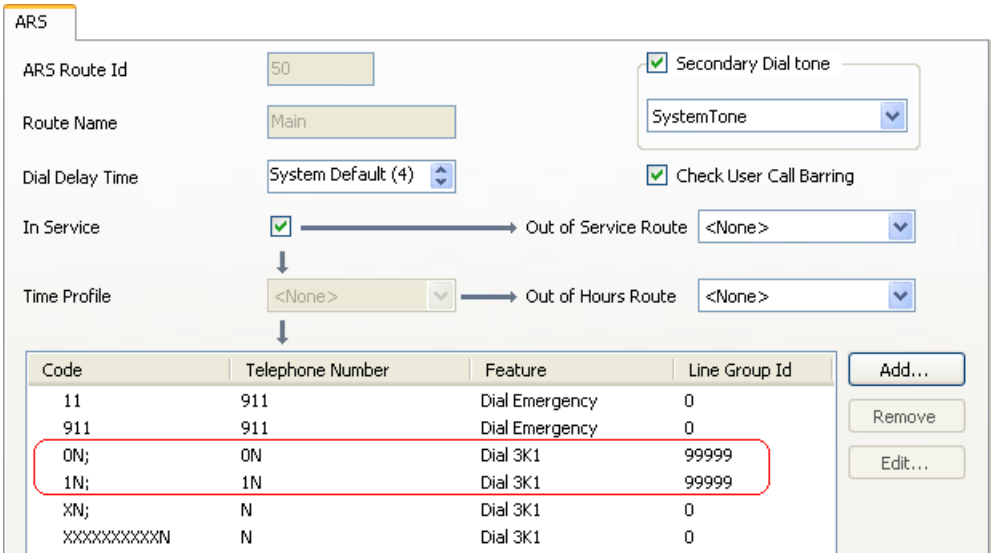
3. Click **50: Main**.



   Within the ARS window, the default **0N;** short code that matches international numbers currently routes those calls to any available trunk in line group 0.

4. To edit the short code, click the short code.
5. Click the **Edit...** button.
6. Make the following changes:
   a. In the **Code** field, leave this set to **0N;**.
   b. In the **Feature** field, change this to **Dial**.
   c. In the **Telephone Number** field, change this to **90N**.

      The **9** has been added back as it matches the dial pattern typically used at the Avaya Aura® site for matching a call that needs routing to the PSTN.
   d. In the **Line Group ID** field, change this to match the Avaya Aura® Session Manager line Outgoing Group ID. The default is **99999**.
7. Click **OK**.
8. Repeat Steps 4 through 7 for the **1N;** short code which is used for national calls. The branch system's default ARS form is now set to route all national and international calls to the Session Manager line and thus to the Avaya Aura® Session Manager.



9. Click **OK**.
10. Select **File > Save Configuration**.

Branch PSTN override

In the example described in Centralized call control on page 289, we configured the branch system so that all national and international calls go to the headquarters site for routing to the PSTN. There may occasionally be scenarios where a particular number needs to override this and be dialed via the branch system's own PSTN trunks.

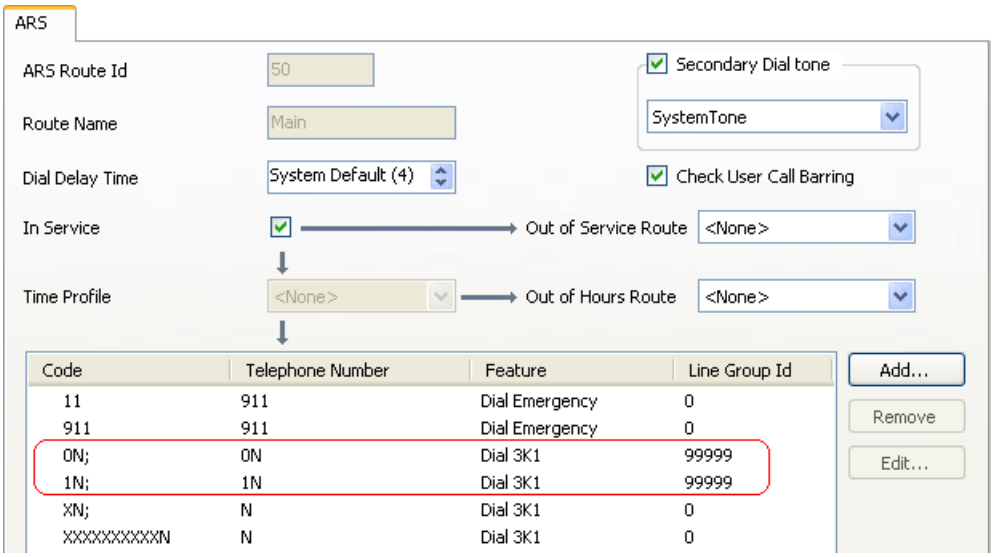
One example is the Avaya Aura Messaging or Modular Messaging PSTN number that can be configured for access to voicemail when the branch's Avaya Aura® Session Manager line is out of service. Another might be to provide a maintenance number to the headquarters site to report suspected loss of the Avaya Aura® Session Manager line connection.

Adding an overriding short code

Procedure

1. From the System Manager console, select the B5800 Branch Gateway device and click **Edit** to edit the system configuration for the device. IP Office Manager will be launched on your PC. For more information, see Editing a B5800 Branch Gateway system configuration from System Manager on page 157.
2. In the left navigation pane, click **ARS**.

3. Click **50: Main**.



Within the ARS form, the default **1N;** short code is the one used for national calls. It would match the MM PSTN Number or AAM PSTN Number and attempt to route it to the SM Line which we know is out of service if the MM PSTN Number or AAM PSTN Number is being used for calls to voicemail. We can change the routing by adding a specific short code for the MM PSTN Number or AAM PSTN Number.

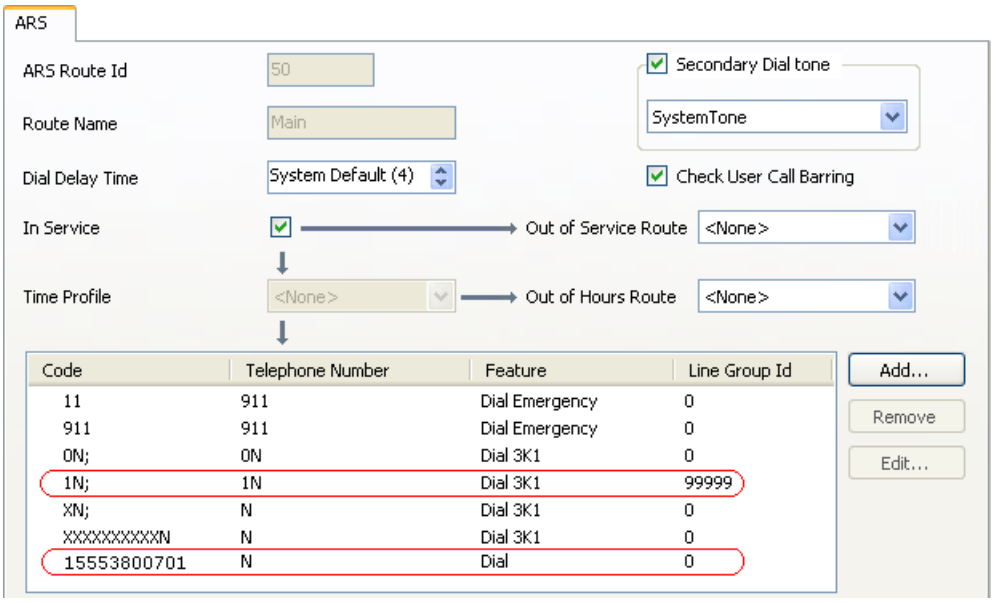
4. To add a short code, click the **Add...** button.
5. Make the changes as follows:
   a. In the **Code** field, set this to match the external PSTN number for Modular Messaging or Avaya Aura Messaging without the external dialing prefix.
   b. In the **Feature** drop-down box, select **Dial3K1**.
   c. In the **Telephone Number** field, set this to **N** to match the whole number in the **Code** field.

      Note:

      For a setup where the voicemail mail box numbers configured on Modular Messaging or Avaya Aura Messaging are the same as the caller's DID, the short code to route the PSTN call should be configured so that the caller ID is withheld. To do this, enter a `W` in the **Telephone Number** field of the short code. This ensures that during rainy-day operation, the voicemail system does not automatically go to the voicemail mail box of the caller based on the caller ID.

   d. In the **Line Group Id** drop-down box, select the line group ID being used for the branch's PSTN trunks. The default is 0.
6. Click **OK**.
   The ARS now has two short codes that will potentially match external national calls. However, one is a more exact match for certain calls and therefore will be applied

to those calls.



7. Click **OK**.
8. Select **File > Save Configuration**.

PSTN trunk fallback

In branch scenarios where centralized call control and trunking (see Centralized call control on page 289) has been configured for certain calls, loss of the Avaya Aura®Session Manager line connection will impact making those calls. For instance, in our example where all branch national and international calls are routed via the headquarters site, loss of the Avaya Aura® Session Manager line will leave the branch users only able to make local calls.

Since loss of the Avaya Aura® Session Manager line should only be an infrequent and temporary condition, some restriction during that state may be acceptable. However the following options can be used to allow continued branch operation:

- If the headquarters site has multiple Avaya Aura®Session Managers for redundancy, each branch can also be configured with multiple Avaya Aura® Session Manager lines. See Avaya Aura Session Manager line redundancy on page 150 for more information.
- As in our example business, centralized call control has not been applied to all branch local calls. Therefore local calls are still available without any additional configuration for the loss of the Avaya Aura® Session Manager line connection.
- Since loss of the Avaya Aura® Session Manager line should be infrequent and temporary, the loss of some services may be tolerable until the Avaya Aura® Session Manager line issue is resolved. However, even if that is the case, it may be recommended to configure

a headquarters PSTN number that can be dialed to report the Avaya Aura® Session Manager line issue. See Branch PSTN override on page 292 for more information.

- Provide PSTN trunk fallback within the branch configuration. See Configuring PSTN trunk fallback on page 295. Note however that PSTN fallback will also occur when the number of external calls exceeds the available SIP trunk licenses.

Note:

If you want to have long distance routing on local trunks, be sure that the appropriate trunks have been ordered from the local provider. Do not create a route for international phone calls if you do not have that service.

Configuring PSTN trunk fallback

About this task

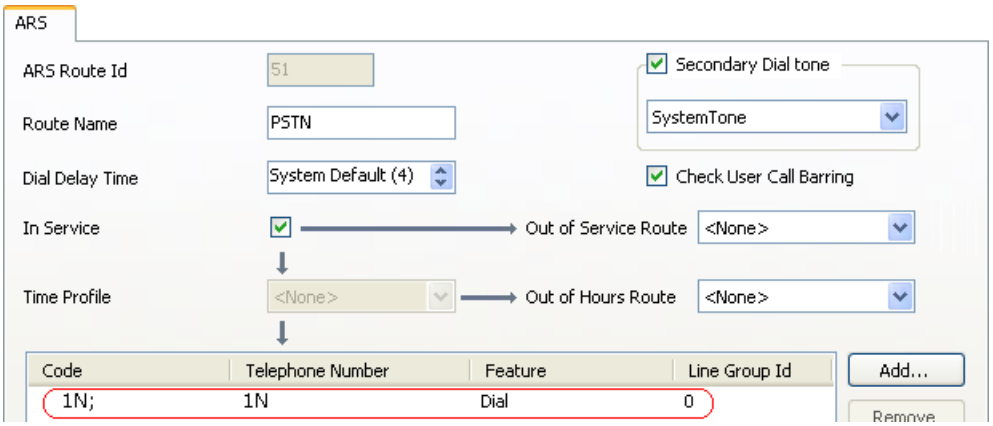
Use this procedure to provide PSTN trunk fallback with the branch configuration.

Procedure

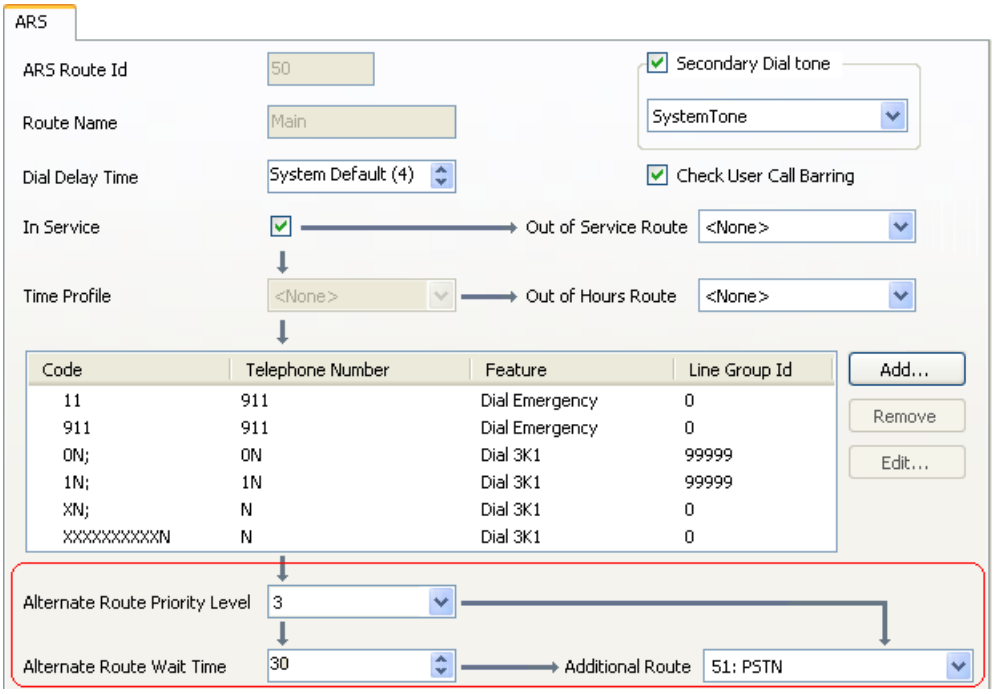
1. Start Manager and connect to the B5800 Branch Gateway system.
2. In the left navigation pane, click **ARS**.
3. Click the **New** icon and select **ARS**.
4. Enter a **Route Name**, for example **PSTN**.
5. To add a short code click the **Add...** button.

   A short code is required that will send the national calls to the branch's own PSTN. Enter the normal defaults for such a short code as follows:
6. Make the changes as follows:
   a. In the **Code** field, enter **1N;**. For this example, **1N;** will match any national number dialing.
   b. In the **Feature** field, leave the entry set as **Dial3K1**.
   c. In the **Telephone Number** field, enter **1N**. For this example **1N** will match the number dialed by the user after the dial 9 prefix.
   d. In the **Line Group Id** drop-down box, select the line group used for the B5800 Branch Gateway system's external trunks. The default is 0.

7. Click **OK**.



8. Click **OK**.
9. Double click on the existing default ARS that was reconfigured to send all branch national and international calls to the Avaya Aura® Session Manager line.



10. In the **Additional Route** drop-down box , select the PSTN ARS form just created above.

    The form is now set such that, if the Avaya Aura® Session Manager line is not available (out of service or all licensed channels busy) calls can be checked for a dialing match in the PSTN ARS form. This works as follows:

    - The **Alternate Route Priority Level** controls which users are able to use the alternate route immediately, ie. those user's whose priority is equal or higher than this setting. The default priority for users is **5**.

- The **Alternate Route Wait Time** is used for caller's whose priority is not sufficient to use the alternate route immediately. The default setting is 30 seconds. However, you may want to adjust this setting to one that meets your requirements.
- Since the only short code match in the alternate route in our example is for national calls, international calls will continue to wait for the Avaya Aura® Session Manager line.

11. Select **File > Save Configuration**.

Appendix D: Authorization codes

Authorization codes are not shown by default. IP Office Manager must be modified in order to support authorization codes. Each authorization code is associated with a particular user or user rights set. The user or users associated with the user rights can then dial numbers which are set to trigger forced authorization code entry. Once a code is entered, the short code settings of the user or user rights with which the code is associated are used to complete the call. This allows authorized users to make otherwise restricted calls from any extension without first having to log in to that extension and then log out after the call.

How authorization codes work

- A user dials a number that matches a short code set to **Force Authorization Code**.
- The user is prompted to enter an authorization code.
- They dial their authorization code. If a matching entry is found in Authorization Codes entries, the system checks the corresponding user or user rights (in that order). Note that the user or user rights checked does not necessarily need to be connected with the user dialing or the user whose extension is being used to make the call.
    - The dial string is checked against the short codes with the matching user or user rights.
    - If it matches a dial short code or no short code, the call is allowed. Otherwise, it is blocked. Note that the short code is not processed, it is just checked for a match.
    - If multi-tier authorization codes are required, there must be blocking (busy) short codes (or a wild card '?')

Example

A restaurant has a number of phones in publicly accessible areas and wants to control what calls can be made from these phones. They want these phones to allow anyone to make local calls, restrict restaurant staff to local and cell phone numbers (044...), and allow the manager to also be able to call long distance numbers (01...). The following table shows how this is configured.

ARS Table	Authorization Codes
In the Main (50) ARS table, the following short codes are added: • *044XXXXXXXXXX / 044N / Dial / Force Auth Code* • *01XXXXXXXXXX / 01N / Dial / Force Auth Code*	The following two authorization codes are configured: • **2008** is associated with a set of **User Rights** called **Cell**. • **1983** is associate with a set of **User Rights** called **LDandCell**.
User Rights	
Cell	**LCandCell**

ARS Table	Authorization Codes
• *044N / . / Dial* Allows calls to cell phone numbers. • *01N / . / Busy* Blocks calls to long distance numbers. • *? / . / Busy* Block any other calls that require an authorization code.	• *044N / . / Dial* Allows calls to cell phone numbers. • *01N / . / Busy* Allows calls to long distance numbers. • *? / . / Busy* Block any other calls that require an authorization code.

It is recommended to use short codes that use X characters to match the full number of characters to be dialed. That ensures that authorization code entry is not triggered until the full number has been dialed rather than mid-dialing. For example, 09 numbers are premium rate in the UK, so you would create a *09XXXXXXXXX / N / Dial* short code set to Forced Authorization. In the associated user or user right short code, it is recommended to use *09N* type short codes.

⚠ Warning:

Changing PC registry settings

Avaya accepts no liability for any issues arising from editing PC registry settings. If you are in any doubt about how to perform this process, you should not proceed. It is your responsibility to ensure that the registry is correctly backed up before any changes are made.

Enabling authorization codes in Manager

About this task

A change to the Manager PC registry settings is required to enable support for authorization codes within Manager. Once this change is made, various authorization code related features are visible when Manager is restarted.

⚠ Warning:

Changing PC registry settings

Avaya accepts no liability for any issues arising from editing PC registry settings. If you are in any doubt about how to perform this process, you should not proceed. It is your responsibility to ensure that the registry is correctly backed up before any changes are made.

Procedure

1. Close Manager.
2. Locate the registry key **HKEY_CURRENT_USER\Software\Avaya \IP400\Manager\EnableAuthorisationCodes** and change its value from **0** to **1**.

3. Restart Manager and load a configuration.

Force authorization codes

There are two methods to force a user to enter an authorization code in order to complete dialing an external call.

- **To Force Authorization Codes on All External Calls**

  A user can be required to enter an authorization code for all external calls. This is done by selecting **Force Authorization Code** (under **User > Telephony > Supervisor Settings**).

- **To Force Authorization Codes on Specific Calls**

  To require entry of an authorization code on a particular call or call type, the **Force Authorization Code** option should be selected in the short code settings. This can be used in user, user rights, or system short codes in order to apply its effect to a user, group of users, or all users respectively. You need to ensure that the user cannot dial the same number by any other method that would by-pass the short code, for example with a different prefix.

About entering an authorization code

Where possible, when an authorization code is required, the user can enter it through their phone's display. However, this is not possible for all types of phones. For example, it is not possible with analog phones and Avaya XX01 or XX02 phones. The users of these devices must enter the authorization code by using a short code set to the Set Authorization Code feature immediately before making the call.

When entry of an authorization code is triggered, the user can enter any authorization code with which they are either directly associated or associated through their current user rights.

Note:

- If account code entry is setup for a particular number, calls forwarded or transferred to that number will also trigger account code entry.
- On systems using line appearances to BRI trunk channels to make outgoing calls, account code entry may not be triggered. This can be resolved by adding a short code such as **[9]XN;/Dial/XN/0** (adjusting the prefix and line group as necessary).

Authorization code configuration settings

- **Authorization Code**: The digits used for the authorization code can be up to 12 digits in length. Each code must be unique. Wild cards are not usable with authorization codes.
- **User Rights**: This field is used to select the user right with which the authorization code is associated. The authorization code can then be used to authorize calls made by users currently associated with that set of user rights.
- **User**: This field is used to select a user with which the authorization code is associated. The authorization code can then be used to authorize calls made by that user.

Appendix E: Recommended courses for Avaya B5800 Branch Gateway training

This appendix lists recommended courses for B5800 Branch Gateway, Session Manager, System Manager, and Communication Manager.

Recommended courses

Table 1: B5800 Branch Gateway

Type	Code	Course title	Delivery	Duration (hours)	First offering
Existing	2U00021O	Avaya Branch Gateway — What Sales needs to know for the first conversation	eLearning	0.5	Available now
Existing	2U00022O	Avaya Branch Gateway — What Sales needs to know to continue the conversation	eLearning	0.5	Available now
Existing	4U00112V	PA Implement: Avaya B5800 Branch Gateway Implementation	vILT	16	Available now
Existing	4U00112A	PA Implement: Avaya B5800 Branch Gateway Implementation Assessment	Online Assessment	1	Available now
New	5U00005V	ACSS — Avaya B5800 Branch Gateway– Implementation, Administration, Maintenance, and Troubleshooting	vILT	40	May 2012
New	TBD	ACSS — Avaya B5800 Branch Gateway– Implementation, Administration, Maintenance, and Troubleshooting Exam	ACSS Proctored Exam	2	May 2012

Table 2: Avaya Aura® Session Manager and System Manager

Type	Code	Course title	Delivery	Duration (hours)	First offering
New	5U00106W	Avaya Aura® System Manager Overview	WBT course	1	Available now
New	5U00105W	Avaya Aura® Session Manager Overview	WBT course	4.5	Available now
New	5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance and Troubleshooting	vILT	16	April 2012
New	5U00096V	Avaya Aura® Session Manager Implementation, Administration, Maintenance and Troubleshooting	vILT	64	April 2012
New	5U00097I	Avaya Aura® Session Manger and System Manager Implementation, Administration, Maintenance and Troubleshooting	ILT	80	April 2012
New	5U00104W	Avaya Aura® Session Manager 6.2 Delta Overview	WBT course	1	Available now
New	5U00103W	Avaya Aura® System Manager 6.2 Delta Overview	WBT course	1	Available now

Table 3: Avaya Aura® Communication Manager and CM Messaging – Embedded

Type	Code	Course title	Delivery	Duration (hours)	First offering
New	5U00041I	Avaya Aura® Communication Manager Administration	ILT	40	Available Now
Existing	3100	Avaya Aura® Communication Manager Administration Exam	ACSS Proctored Exam	1	Available Now
Existing	5U00040I	Avaya Aura® Communication Manager Maintenance and Troubleshooting	ILT	40	Available Now
Existing	5M00050I/V	Avaya Aura® Communication Manager Messaging Embedded Administration, Maintenance and Troubleshooting	vILT/ILT	40	Available Now

Type	Code	Course title	Delivery	Duration (hours)	First offering
Existing	3101	Avaya Aura® Communication Manager and CM Messaging - Embedded Maintenance and Troubleshooting Exam	ACSS Proctored Exam	1.75	Available Now
Update	ATI02348IEN/VEN	Avaya Aura® Communication Manager Implementation	vILT/ILT	40	March 2012
Existing	ATI01731VEN	Avaya Aura® Communication Manager Messaging Embedded Implementation	vILT	16	Available Now
New	4U00115I/V	Avaya Aura® Communication Manager Implementation Upgrade (R5.X to R6.X)	vILT/ILT	16	March 2012
Existing	6002	Avaya Aura® Communication Manager and CM Messaging (R6.X) Implementation Exam	ACIS Proctored Exam	2	Available Now
New	4U00121W	Avaya Aura® Communication Manager 6.2 Technical Delta	WBT course	2	Available Now

Glossary

Centralized management	This term is used to describe a central management system that delivers a set of shared management services and provides a single access interface to administer multiple branch locations and multiple distributed B5800 Branch Gateway users.
Centralized trunking	This term describes routing outgoing external calls from the branch sites to the central site in order to utilize the central sites PSTN trunks. The same applies for distributing incoming PSTN calls from the central site to the appropriate branches.
Distributed Branch user model	This term describes a B5800 Branch Gateway deployment model where call processing for the branch phones is provided locally. Non-IP phones are connected to B5800 Branch Gateway and IP and certain SIP endpoints (not including the Avaya 9600 SIP phones) can be administered with B5800 Branch Gateway as their controller. Access to and from the rest of the Avaya Aura® network is via the B5800 Branch Gateway system's Avaya Aura®Session Manager link across the enterprise WAN. This connection allows for VoIP connectivity to other B5800 Branch Gateway systems, to centralized trunking and to centralized applications such as conferencing and Modular Messaging.
Distributed trunking	This term describes the scenario where each branch retains and uses its own PSTN trunks for incoming and outgoing external calls.
Local extension	See Native extension.
Local management	This term is used to describe managing a B5800 Branch Gateway device using the local IP Office Manager application.
Mixed mode trunking	The flexibility of Avaya Aura® Session Manager is such that both centralized and distributed trunking can be used. For example, routing all national and international calls via centralized trunking at the headquarters site while still allowing local calls via the branch sites.
Native extension	This term is used to describe extensions that get their call services from the branch site and operate in the Distributed Branch user model. A native extension is also referred to as a local extension.
Rainy day	This term refers to a loss of network connectivity from the branch to the core data center.
Sunny day	This term refers to full network connectivity from the branch to the core data center.

Tail-End-Hop-Off Part of mixed mode trunking, this describes scenarios where certain calls at other branches or the headquarters site are routed to the PSTN of another branch.

Index

A

About adding B5800 Branch Gateways to System Manager 125
About the xml file containing the B5800 Branch Gateway devices 129
About upgrading B5800 Branch Gateway software ...16
activating license entitlements 191
Activating license files 115
activation process 190
Adding distributed users to System Manager 185
additional system procedures 203
Administering users 185
  centralized users 185
  distributed users 185
Alternate Route Priority Level 294
Alternate Route Wait Time 294
Analog 75
  phone barrier boxes 75
ARS 294
Audio 44
  codec conversion 44
Authorization code configuration settings 302
Authorization codes 299
Automatic codec preference settings 144
Avaya Mentor videos 31

B

B5800 Branch Gateway administration tools 199
  using SAL to access 199
B5800 Branch Gateway licenses 18
B5800 upgrades 98
Barrier boxes 75, 76
  analog phone 75
  rack mounting 76
Batteries 264
  Lithium 264
branch and extension numbering 140
bulk import of users 93
Bulk importing of devices 128

C

Cable 48
  access requirements 48
  clearance requirements 48
Cables 42
  Maximum cable distances 42
  Standard IP Office 42
Cabling 72
  lightening protection 72
Call flows 287
Castle Rock 224
Centralized call control 289
change history 33
Channels 44
  compression 44
Clock 135
Compression channels 44
Configuration 57, 231
  create new 57
  erase 231
configuration checklist 109
Configuring Avaya Aura Messaging 176
configuring Embedded Voicemail 173
Configuring Modular Messaging 178
configuring Standalone Voice Mail 174
configuring the B5800 Branch Gateway for certificates 123
configuring user PLDS access 101
Connecting the control unit to the network 86
Connections 44, 72
  grounding 44
  out of building 72
Control unit 44
  Rack mounting 44
  wall mounting 44
Country 27
  languages 27
  supported locales 27
Create configuration file 57
creating a backup of the system configuration using System Manager 215
Creating a software library 102
creating a system template 131
creating a user template 133

D

Default codec selection 143
deleting license files from the branches 95
Deliver activated license files to the branches 117

Dial pattern 170
Disabling the System Manager administration feature for a branch 159
discovering branches in the network and adding them to System Manager 126
Domain 166
DS 74
IROB 74
phone 74
DTE port 230
Cable requirement 230
RS232 230
settings 230

E

editing a B5800 Branch Gateway from System Manager 157
editing the B5800 Branch Gateway Endpoint profile for a user 187
editing the xml file containing the users 92
egress ports for B5800 Branch Gateway and SIP phones 281
EMC Cautions 266
Canadian Department of Communications 266
EMC Caution for China 266
Federal Communications Commission 266
Enabling authorization codes in Manager 300
Enabling branch SIP extension support 154
enabling secure communication after upgrading IP Offfice Manager 91
Enabling WebLM licensing for the branch 130
Entity link 168
Envirmental requirements 47
Example of So8 BRI module configuration 221
exporting users to an xml file 92
EXT O/P Port 220
Extension numbers 212, 213
changing 213
Renumbering 213
swapping 212
external server 98

F

Fallback 294
FCC Rules 272
firewall policies 278
firewall types 277
Force authorization codes 301
FQDN 167

G

General information 31
training courses 31
generating a certificate on System Manager 119
Getting inventory 100
ggeneral information 32
Web sites 32
Grounding control units 44

H

Hazard Symbols 264
Homologation Statement 263
Hop-Off 38, 289
how ports are used 275
HP OpenView 224

I

ingress ports for B5800 Branch Gateway and SIP phones 279
initial branch configuration 109
Initial Installation Utility 121
Initial Installation Utility, features automatically configured 123
installation 53
Installation 54, 55, 59, 65, 67, 71, 79
admin applications 79
card 59
grounding 71
installer PC connection 79
rack mounting 67
tools 54
unpacking 55
wall mounting 65
installation checklist 53
installing a service pack 97
Installing IP Office Manager Lite from the System Manager server to a PC 114
installing the license file on the System Manager WebLM server 117
IP Address 167
IP Office Operation in 270
USA 270

L

legal notices 2
license entitlements 191, 193

activating 191
searching for 193
license modes 19
Licensing 16
Lightening Portection 264
Lightening protection 72
Link Monitoring 167
Lithium Batteries 264
Location, adding 166

M

management 14
Manager 134–137, 213, 216
clock quality 135
extension numbers 213
prefix dialing 137
trunk clock quality setting 136
trunks 134
upgrade software 216
Managing B5800 Branch Gateways from System Manager 157
manually adding B5800 Branch Gateways to System Manager 129
Maximum SIP sessions 144
migrating individual PLDS license files to a WebLM server 94
Module 222
Polycom video 222
Modules 265
Trunk Interface 265
Monitoring 167

N

network assessment for VoIP requirements 39
New configuration 57
new in this release 29

O

Operation in 267–270
Australia 267
Canada 268
China 269
European Union 270
New Zealand 270
Out of building 72
connections 72
outgoing call routing 151

P

Park and Page 172
Pattern 170
Planning 35
PLDS 189, 190
about 189
Policy 169
Polycom video module 222
Port 168, 219, 220, 230, 265
door 219
EXT O/P 220
RS323 DTE 230
Safety Classification 265
port matrix for B5800 Branch Gateway and SIP phones 275
port type ranges 275
port usage diagram 285
Power Supplies 41
Uninterrupted Power Supply 41
prerequisites 35
Prerequisites 35
Protocol 168
PSTN trunk fallback 294
PSTN trunk fallback, configuring 295
PSTN trunking configurations 13

R

R6.2 service pack installation checklist 97
Rack mounting control units 44
Recommended courses 303
Redundancy 150
regenerate license files 197
regenerating a license file 197
registering 190
rehosting 195
related documents 31
related resources 31
Avaya Mentor videos 31
remote software library 98, 99
remote software library for B5800 upgrades 98
Renumber extensions 213
Requirements 47, 48
Cable access 48
Cable clearance 48
Enviromental 47
space 48
Wall mounting 47
reset button 238
restoring the system configuration using System Manager 218

Restrictions when editing a B5800 Branch Gateway system configuration from System Manager 158
revision history 33
Routing B5800 Branch Gateway calls 290
Routing policy 169

S

Safety instructions 263
Safety statements 263
SAL 199–201
alarming 201
registration 201
registration request form 201
standalone gateway 199, 200
searching for license entitlements 193
sending the system template to multiple B5800 Branch Gateways 132
Session Manager tab field descriptions 146
Setting B5800 Branch Gateway SNMP attributes 100
setting up external server 99
Setting up System Manager to launch IP Office Manager 112
setting up the external server as remote software library 99
Short Code tab field descriptions 153
SIP domain 166
SIP entity 168
SIP Link Monitoring 167
SIP Registrar tab field descriptions 155
SIP trunk support 139
SM line redundancy 150
SNMP 127, 224, 225, 228, 229
enabling 127, 228
installation 225
port 127, 228
respond 127, 228
trap sending 229
So8 ....221, 222
example ISDN terminal 221
Example video conference 222
sockets 276
Software 235
erasecore software 235
Software applications 26
Space requirements 48
Statement 263
Homologation 263
Safety 263
Supported 27
language 27
locales 27
supported telephones 23
Synchronizing B5800 Branch Gateway with System Manager 162
System components 20
System Manager administration feature, disabling from IP Office Manager 160
System Manager administration feature, disabling using System Manager 160
system requirements 98
system requirements for the external server 98
System shutdown using Manager 206
System tab field descriptions 141

T

Tail-End-Hop-Off 38, 289
TFTP port usage 278
Time range, adding 169
Training 303
Training courses 31
Trunk fallback 294
Trunk Interface Modules 265
Trusted 168
Type 167
types of activation process 190

U

upgrade installation 89
upgrade installation checklist 89
upgrading the administration applications 90
upgrading the B5800 Branch Gateway device 103
Uploading an auto attendant audio file 132, 182
using Embedded File Management to install a PLDS license 118

V

videos 31
Avaya Mentor 31
Voice compression channels 44
Voicemail considerations 37
Voicemail operation 171
Voicemail support options 14
VoIP tab field descriptions 147

W

Wall mounting control units 44
Wall mountingrequirements 47
WAN 239

link 239
Web sites 32